Journal of Algebra 353 (2012) 261–285

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Closest multiplication tables of groups ☆

Petr Vojtěchovský [a,*], Ian M. Wanless [b]

[a] Department of Mathematics, University of Denver, CO 80208, USA
[b] School of Mathematical Sciences, Monash University, VIC 3800, Australia

ARTICLE INFO

Article history:
Received 2 March 2011
Available online 4 January 2012
Communicated by Derek Holt

MSC:
05B15
20D60

Keywords:
Group multiplication table
Hamming distances of groups
Rainbow matching

ABSTRACT

Suppose that all groups of order n are defined on the same set G of cardinality n, and let the *distance* of two groups of order n be the number of pairs $(a,b) \in G \times G$ where the two group operations differ. Given a group $G(\circ)$ of order n, we find all groups of order n, up to isomorphism, that are closest to $G(\circ)$.

1. Introduction

Let G be a finite set of cardinality n, and let $\circ, *, \cdot, \bullet$ be group operations defined on G. For groups $G(\circ)$, $G(*)$, let

$$\operatorname{diff}(\circ,*) = \big\{(a,b) \in G \times G;\ a \circ b \neq a * b\big\},$$
$$\operatorname{dist}(\circ,*) = \big|\operatorname{diff}(\circ,*)\big|,$$

and call $\operatorname{dist}(\circ,*)$ the (*Hamming*) *distance of groups* $G(\circ)$, $G(*)$.

☆ This work was partially supported by a grant from the Simons Foundation (grant 210176 to Petr Vojtěchovský) and by the Australian Research Council (grants DP0662946 and DP1093320 to Ian Wanless).

* Corresponding author.
E-mail addresses: petr@math.du.edu (P. Vojtěchovský), ian.wanless@monash.edu (I.M. Wanless).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.11.026

In a research programme spanning two decades, Aleš Drápal showed that there is a strong relationship between algebraic properties of groups and their distances, as will become apparent from many of his results we quote below.

In this paper we solve the following problem: *Given a group $G(\circ)$, determine all multiplication tables of groups $G(*)$ (up to isomorphism) that are as close to the multiplication table of $G(\circ)$ as possible.* More formally, let

$$\delta(\circ) = \min\bigl\{\operatorname{dist}(\circ,*);\ G(\circ) \neq G(*)\bigr\},$$
$$\Delta(\circ) = \bigl\{G(*);\ \operatorname{dist}(\circ,*) = \delta(\circ)\bigr\}.$$

Our task is then to find $\delta(\circ)$ and to construct one group $G(*)$ of minimum distance from $G(\circ)$ for every isomorphism class of groups intersecting $\Delta(\circ)$.

In particular, we determine the minimal distance

$$\delta(n) = \min\bigl\{\delta(\circ);\ G(\circ) \text{ is a group of order } n\bigr\}$$

and all pairs of groups $G(\circ)$, $G(*)$ (up to isomorphism) of order n satisfying $\operatorname{dist}(\circ,*) = \delta(n)$.

1.1. The context

Let

$$\delta_{\cong}(\circ) = \min\bigl\{\operatorname{dist}(\circ,*);\ G(\circ) \cong G(*) \neq G(\circ)\bigr\},$$
$$\delta_{\ncong}(\circ) = \min\bigl\{\operatorname{dist}(\circ,*);\ G(\circ) \ncong G(*)\bigr\},$$

where the second quantity is set to ∞ if all groups of order n are isomorphic. Obviously, we have $\delta(\circ) = \min\{\delta_{\cong}(\circ), \delta_{\ncong}(\circ)\}$.

An important threshold for $\delta(\circ)$ is obtained by considering pairs of groups isomorphic via a transposition. Note that if $f = (a, b)$ is an isomorphism between $G(\circ)$ and $G(*)$ then $\operatorname{diff}(\circ,*)$ is a subset of the rows and columns indexed by a, b, and of the "diagonal" entries (x, y) with $x \circ y \in \{a, b\}$. This means that $\delta(n)$ will not exceed $6n$. More precisely:

As in [3], for a nontrivial commutative group O of odd order, let $D(O)$ be the generalized dihedral group defined on $O \times C_2$ by

$$(a,0)(b,h) = (ab,h), \qquad (a,1)(b,h) = \bigl(ab^{-1}, 1+h\bigr).$$

Then let

$$\delta_0(\circ) = \begin{cases} 6n-18, & \text{if } n \text{ is odd},\\ 6n-20, & \text{if } G(\circ) \cong D(O) \text{ for some } O,\\ 6n-24, & \text{otherwise.}\end{cases} \tag{1.1}$$

The main results of [3] can be summarized as follows:

Theorem 1.1 *(Drápal). Let $|G| = n$ and let $G(\circ)$, $G(*)$ be groups defined on G. If $\operatorname{dist}(\circ,*) < n^2/9$ then $G(\circ)$ and $G(*)$ are isomorphic. If $n \geqslant 5$ then $\operatorname{dist}(\circ,*) \geqslant \delta_0(\circ)$ whenever $G(*)$ is isomorphic to $G(\circ)$ via a transposition, and $\operatorname{dist}(\circ,*) = \delta_0(\circ)$ for some $G(*)$ isomorphic to $G(\circ)$ via a transposition. Consequently, if $n \geqslant 51$ then $\delta(\circ) = \delta_0(\circ) = \delta_{\cong}(\circ) < \delta_{\ncong}(\circ)$.*

Moreover, [3, Proposition 5.8] describes in detail the transpositions that achieve the distance $\delta_0(\circ)$. Hence our problem has already been solved in all but finitely many cases. Here is an overview of other known results concerning distances of groups:

To determine $\delta_{\not\cong}(\circ)$ appears to be a very difficult problem. We already know from Theorem 1.1 that $\delta_{\not\cong}(\circ) \geqslant n^2/9$ whenever $n \geqslant 5$. When $G(\circ)$ is a 2-group then $\delta_{\not\cong}(\circ) \geqslant n^2/4$ by [4]. Examples of non-isomorphic 2-groups at *quarter distance*, that is, with $\operatorname{dist}(\circ, *) = n^2/4$, can be found in [8] and [9]. In [5], Drápal constructed a family of p-groups for every prime $p > 2$ with the property $\delta_{\not\cong}(\circ) = (n^2/4)(1 - 1/p^2)$. In particular, there is a 3-group satisfying $\delta_{\not\cong}(\circ) = 2n^2/9$ (see also Construction 2 in Section 11.2). Ivanyos et al. [13] showed, after this paper had been submitted, that $\delta_{\not\cong}(\circ) \geqslant 2n^2/9$ always holds.

Let $\mathcal{G}(n)$ be a graph whose vertices are the isomorphism classes of groups of order n, and in which two vertices, possibly the same, form an edge if and only if they contain representatives at distance $\delta(n)$.

When n is a power of two, let $\mathcal{G}'(n)$ be a graph on the same vertices as $\mathcal{G}(n)$ in which two vertices, possibly the same, form an edge if an only if they contain representatives at distance $n^2/4$ obtained by one of the two constructions of Drápal [8] that we recall in Section 11.1. When $n \in \{8, 16\}$, it turns out that $\delta(n) = n^2/4$, so $\mathcal{G}'(n)$ is a subgraph of $\mathcal{G}(n)$.

By [6], $\delta(\circ) \geqslant n^2/4$ for any 2-group $G(\circ)$ of order $n \leqslant 16$. In [17,18], the first author determined the connected graph $\mathcal{G}(8)$ with $\delta(n) = 8^2/4 = 16$ (we checked that $\mathcal{G}'(8) = \mathcal{G}(8)$), calculated $\delta(\circ)$ for cyclic groups $G(\circ)$ of order less than 13, proved that $\delta(\circ) = 6n - 18$ whenever $G(\circ)$ is a group of prime order $n > 7$, and constructed a class of groups with $\delta(\circ) < \delta_0(\circ)$, of which the largest member has order 21. (As we are going to show, $n = 21$ happens to be the largest order for which $\delta(\circ) < \delta_0(\circ)$ can occur.)

Bálek [1] computed the subgraph $\mathcal{G}'(16)$ (excluding the diagonal entries) of $\mathcal{G}(16)$. Since $\mathcal{G}'(16)$ turns out to be connected, it follows that $\delta(\circ) = n^2/4$ for every group $G(\circ)$ of order $n = 16$. A more direct argument establishing the connectedness of $\mathcal{G}(16)$ can be found in [11]. Our computational results show that $\mathcal{G}'(16) = \mathcal{G}(16)$. The two constructions of Section 11.1 can therefore be seen as canonical for $n \in \{8, 16\}$.

Groups at quarter distance received attention even for orders $n = 2^k > 16$, although then $\delta(n) < n^2/4$ so $\mathcal{G}'(n)$ is no longer a subgraph of $\mathcal{G}(n)$. In [20], Zhukavets calculated $\mathcal{G}'(32)$ and $\mathcal{G}'(64)$; the first graph is connected while the second one has two connected components.

The quarter distance is of interest outside the variety of groups, too. In [10], Drápal and the first author generalized the constructions of [8] for *Moufang loops*, that is, loops satisfying the identity $x(y(xz)) = ((xy)x)z$. The first author went on to construct a large family of Moufang loops of order 64 [19], starting with the well-known Moufang loops $M_{2n}(G, 2)$ of Chein [2, pp. 35–38] and using the constructions of [10]. Nagy and the first author eventually proved in [16] that the family of [19] actually contains all Moufang loops of order 64 up to isomorphism.

Distances of infinite groups are somewhat trivial, as it was shown in [3] that if $G(\circ)$ is a group of infinite cardinality κ then $\delta_{\cong}(\circ) = \delta_{\not\cong}(\circ) = \kappa$.

1.2. The content

For the convenience of the reader, the main result is stated at the outset in Section 2.

For two subsets $\mathcal{A}$, $\mathcal{B}$ of groups defined on G, let

$$\operatorname{dist}(\mathcal{A}, \mathcal{B}) = \min\bigl\{\operatorname{dist}(\circ, *);\ G(\circ) \in \mathcal{A},\ G(*) \in \mathcal{B},\ G(\circ) \neq G(*)\bigr\}.$$

Denote by $[\circ]$ the class of all groups defined on G and isomorphic to $G(\circ)$. In Section 3, we recall that $\operatorname{dist}([\circ], [*]) = \operatorname{dist}([\circ], *)$. Consequently, the values of $\delta(\circ)$, $\delta_{\cong}(\circ)$ and $\delta_{\not\cong}(\circ)$ depend only on the isomorphism type of $G(\circ)$. If $n \geqslant 5$, Lemma 3.3 allows us to assume that closest groups have the same neutral element. Lemma 3.4 shows how automorphism groups of $G(\circ)$, $G(*)$ come into play to speed up the calculation of $\operatorname{dist}([\circ], [*])$.

In Section 4 we introduce, following Drápal, these concepts and parameters:

$$\begin{aligned}
&\operatorname{diff}_a(\circ,*) = \big\{(a,b);\ b\in G,\ a\circ b\neq a*b\big\}, \qquad \operatorname{dist}_a(\circ,*) = \big|\operatorname{diff}_a(\circ,*)\big|,\\
&m(\circ,*) = \min\big\{\operatorname{dist}_a(\circ,*);\ a\in G,\ \operatorname{dist}_a(\circ,*)>0\big\},\\
&H(\circ,*) = \big\{a\in G;\ \operatorname{dist}_a(\circ,*)=0\big\}, \qquad h(\circ,*) = \big|H(\circ,*)\big|,\\
&K(\circ,*) = \big\{a\in G;\ \operatorname{dist}_a(\circ,*)<n/3\big\}, \qquad k(\circ,*) = \big|K(\circ,*)\big|.
\end{aligned} \tag{1.2}$$

When $\circ$, $*$ are fixed, we drop the operations from the names of the parameters and write dist_a, m, H, and so on.

Among other results, we recall in Section 4 that $a\circ b\neq a*b$ implies $\operatorname{dist}_a+\operatorname{dist}_b+\operatorname{dist}_{a\circ b}\geqslant n$; the set H is either empty or it is a subgroup of both $G(\circ)$ and $G(*)$; if $|k|>3n/4$ then $\operatorname{dist}(\circ,*)>\delta_0(\circ)$; $m\geqslant 2$ if n is even and $m\geqslant 3$ if n is odd. We also study dist_a when the orders of a in $G(\circ)$ and $G(*)$ disagree.

Building on these results, in Section 5 we develop a series of inequalities relating n, h, k, m and, consequently, we find only a few (less than hundred) quadruples (n,h,k,m) in the range $22<n<51$ that can possibly yield $\operatorname{dist}(\circ,*)\leqslant\delta_0(\circ)$. This will already imply that $\operatorname{dist}(\circ,*)<\delta_0(\circ)$ cannot hold for $n\geqslant 43$, improving upon the bound $n\geqslant 51$ of Theorem 1.1.

In Section 6, we first show that the case $m=2$ can be reduced to the study of distances of the cyclic group C_n from a group possessing an element of order $n/2$, a case that is not difficult to handle computationally. We can proceed similarly when n is a prime, independently verifying the results of [17,18].

The general algorithm for finding $\operatorname{dist}([\circ],[*])$ is given in Section 7. The algorithm is sufficiently fast to deal with all orders $n\leqslant 22$ and also all cases when $h>1$, leaving us with only 20 quadruples (n,h,k,m), which require a very delicate analysis.

In Section 8 we study the question: *Given an edge-colored graph on v vertices such that no color is used more than m times and no vertex is adjacent to more than two edges of the same color, how many edges must the graph have to guarantee a rainbow i-matching?* A partial answer can be found in Proposition 8.1.

Returning to the problem of group distances, in Section 9 we study the set $\{(a,b)\in\operatorname{diff}(\circ,*);\ a\in K,\ b\notin K,\ a\circ b\notin K\}$ and similar sets which give rise to edge-colored graphs. The main idea of Section 9 is to exhibit a large enough rainbow matching in a certain graph to push the distance over the threshold $\delta_0(\circ)$.

Only 7 quadruples (n,h,k,m) remain after this analysis, all with $n\leqslant 28$. These are disposed of in Section 10, using a series of increasingly more specialized lemmas.

Finally, in Section 11 we present several constructions that produce all pairs $G(\circ)$, $G(*)$ with $\operatorname{dist}(\circ,*)=\delta(\circ)<\delta_0(\circ)$. These are the constructions alluded to in Theorem 2.1, the main result.

2. Main result

Theorem 2.1. *Let G be a set of size $n\geqslant 4$. Let $G(\circ)$ be a group defined on G, $\delta(\circ)=\min\{\operatorname{dist}(\circ,*);\ G(*)$ is a group different from $G(\circ)\}$, $\Delta(\circ)=\{G(*);\ \operatorname{dist}(\circ,*)=\delta(\circ)\}$, and let $\delta_0(\circ)$ be defined as in* (1.1).

Then the value of $\delta(\circ)$ and one representative from $\Delta(\circ)$ for every isomorphism type of groups present in $\Delta(\circ)$ can be found as follows:

- *If $n\notin\{4,6,7,8,9,10,12,14,15,16,18,21\}$ then $\delta(\circ)=\delta_0(\circ)$, all groups in $\Delta(\circ)$ are isomorphic to $G(\circ)$, and there is a transposition f of G such that $f: G(\circ)\to G(*)$ is an isomorphism and $G(*)\in\Delta(\circ)$.*
- *Otherwise the value of $\delta(\circ)$ and the isomorphism types of groups in $\Delta(\circ)$ can be found in Table* 1. *When n is a power of two and also in the case $\operatorname{dist}(C_3\times S_3, C_3\times S_3)$, the representatives of $\Delta(\circ)$ can be obtained by the constructions of Section* 11.1. *When n is not a power of two, the representatives of $\Delta(\circ)$ can be obtained by one of the three types of constructions of Section* 11.2, *as indicated by the superscript in the table.*

Table 1
Distances of isomorphism classes of groups for all orders n where at least one group $G(\circ)$ satisfies $\delta(\circ) < \delta_0(\circ)$. A group of order n labeled by i is the ith group of order n as listed in GAP. The row labels are structural descriptions of the groups with the usual conventions. The distance $\mathrm{dist}([\circ],[*])$ between the ith group $G(\circ)$ and the jth group $G(*)$ of order n can be found in row i and column j of the table for n. This value is underlined if it is less than $\delta_0(\circ)$ (this has the potential to break the diagonal symmetry of the tables but actually never does), it is in bold face if it equals $\delta(n)$, and it is replaced with "?" if it was not calculated exactly but exceeds $\delta_0(\circ)$. The superscript points to a construction in Section 11.2 that achieves the distance.

$n=4$	1	2
$C_4=1$	7	**4**
$(C_2)^2=2$	**4**	16

$n=6$	1	2
$S_3=1$	16	12^1
$C_6=2$	12	$\underline{\mathbf{8}}^2$

$n=9$	1	2
$C_9=1$	$\underline{\mathbf{18}}^3$	$\underline{\mathbf{18}}^2$
$(C_3)^2=2$	$\underline{\mathbf{18}}^2$	36

$n=7$	1
$C_7=1$	$\underline{\mathbf{18}}^3$

$n=15$	1
$C_{15}=1$	$\underline{\mathbf{50}}^2$

$n=10$	1	2
$D_{10}=1$	40	40^1
$C_{10}=2$	40	$\underline{\mathbf{24}}^2$

$n=14$	1	2
$D_{14}=1$	64	84
$C_{14}=2$	84	$\underline{\mathbf{48}}^2$

$n=21$	1	2
$C_7\rtimes C_3=1$	108	?
$C_{21}=2$	?	$\underline{\mathbf{98}}^2$

$n=8$	1	2	3	4	5
$C_8=1$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	24	24	28
$C_4\times C_2=2$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$
$D_8=3$	24	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$
$Q_8=4$	24	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	24	24
$(C_2)^3=5$	28	$\underline{\mathbf{16}}$	$\underline{\mathbf{16}}$	24	24

$n=12$	1	2	3	4	5
$\mathrm{Dic}_3=1$	$\underline{\mathbf{32}}^2$	48	82	$\underline{36}$	60
$C_{12}=2$	48	$\underline{\mathbf{32}}^2$	70	60	$\underline{36}$
$A_4=3$	82	70	48	72	60
$D_{12}=4$	$\underline{36}$	60	72	$\underline{\mathbf{32}}^2$	48
$C_6\times C_2=5$	60	$\underline{36}$	60	48	$\underline{\mathbf{32}}^2$

$n=18$	1	2	3	4	5
$D_{18}=1$	$\underline{\mathbf{72}}^3$	144	144	$\underline{\mathbf{72}}^2$	180
$C_{18}=2$	144	$\underline{\mathbf{72}}^3$	138	180	$\underline{\mathbf{72}}^2$
$C_3\times S_3=3$	144	138	$\underline{81}$	108	108
$(C_3)^2\rtimes C_2=4$	$\underline{\mathbf{72}}^2$	180	108	88	144
$C_6\times C_3=5$	180	$\underline{\mathbf{72}}^2$	108	144	$\underline{\mathbf{72}}^2$

$n=16$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$C_{16}=1$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	112	112	$\underline{\mathbf{64}}$	96	112	112	112	112	136	136	128	148
$(C_4)^2=2$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88	128	112	112	$\underline{\mathbf{64}}$	96	96	96	112
rank 2 $(C_4\times C_2)\rtimes C_2=3$	112	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88	$\underline{\mathbf{64}}$	96	$\underline{\mathbf{64}}$	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	96	96
$C_4\rtimes C_4=4$	112	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88	$\underline{\mathbf{64}}$	96	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	112
$C_8\times C_2=5$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88	88	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	96	96	$\underline{\mathbf{64}}$	96	96	96	112
$C_8\rtimes C_2=6$	96	88	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	96	96	88	96	96	$\underline{\mathbf{64}}$	128
$D_{16}=7$	112	128	96	96	96	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	112	$\underline{\mathbf{64}}$	112	96	112
$QD_{16}=8$	112	112	$\underline{\mathbf{64}}$	96	96	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	112	96	96	$\underline{\mathbf{64}}$	128
$Q_{16}=9$	112	112	96	$\underline{\mathbf{64}}$	96	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	112	96	$\underline{\mathbf{64}}$	96	136
$C_4\times(C_2)^2=10$	112	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88	112	112	112	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$
$C_2\times D_8=11$	136	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	96	$\underline{\mathbf{64}}$	96	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$
$C_2\times Q_8=12$	136	96	96	$\underline{\mathbf{64}}$	96	96	112	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96
rank 3 $(C_4\times C_2)\rtimes C_2=13$	128	96	96	96	96	$\underline{\mathbf{64}}$	96	$\underline{\mathbf{64}}$	96	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	88
$(C_2)^4=14$	148	112	96	112	112	128	112	128	136	$\underline{\mathbf{64}}$	$\underline{\mathbf{64}}$	96	88	72

In particular,

- $\delta(\circ) < \delta_0(\circ)$ *if and only if* $G(\circ)$ *is one of the following groups*: C_6, C_{10}, C_{14}, C_{21}, *a group of order* 12 *except for* A_4, *a group of order* 7, 8, 9, 15, 16 *or* 18.

- $\Delta(\circ)$ *contains groups of more than one isomorphism type if and only if* $G(\circ)$ *is one of the following groups*: C_9, D_{10}, *a group of order* 8, *a group of order* 16, D_{18}, C_{18}, $C_6 \times C_3$.
- $\Delta(\circ)$ *contains no groups isomorphic to* $G(\circ)$ *if and only if* $G(\circ)$ *is one of the following groups*: C_4, $(C_2)^2$, S_3, Q_8, $(C_2)^3$, $(C_3)^2$, $(C_2)^4$, $(C_3)^2 \rtimes C_2$.

2.1. Additional results

The values $\delta_{\cong}(C_n)$ for $4 \leqslant n \leqslant 22$ are as follows:

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\delta_{\cong}(C_n)$	7	12	8	18	16	18	24	48	32	60	48	50	64	84	72	96	96	98	108

The distances for $n \in \{20, 22\}$ are as follows, with the same notational conventions as in Table 1:

$n = 20$	1	2	3	4	5
$\mathrm{Dic}_5 = 1$	**96**	?	?	100	?
$C_{20} = 2$	?	**96**	?	?	100
$C_5 \rtimes C_4 = 3$	?	?	**96**	?	?
$D_{20} = 4$	100	?	?	**96**	160
$C_{10} \times C_2 = 5$	?	100	?	160	**96**

$n = 22$	1	2
D_{22}	112	?
C_{22}	?	**108**

3. Distances of isomorphism classes

For a group $G(\circ)$ and a bijection $f : G \to G$ there is a unique group $G(*)$ such that $f : G(\circ) \to G(*)$ is an isomorphism, namely $a * b = f(f^{-1}(a) \circ f^{-1}(b))$. We denote this operation $*$ by $\circ_f$.

Lemma 3.1. *Let* $G(\circ)$, $G(*)$ *be groups and* $f : G \to G$ *a bijection. Then* $\mathrm{dist}_a(\circ, *) = \mathrm{dist}_{f(a)}(\circ_f, *_f)$ *for every* $a \in G$. *In particular,* $\mathrm{dist}(\circ, *) = \mathrm{dist}(\circ_f, *_f)$.

Proof. Fix $a \in G$. The cardinalities of the sets of elements $b \in G$ satisfying any of the following conditions are the same:

$$a \circ b \neq a * b,$$
$$f^{-1}\big(f(a)\big) \circ b \neq f^{-1}\big(f(a)\big) * b,$$
$$f^{-1}\big(f(a)\big) \circ f^{-1}(b) \neq f^{-1}\big(f(a)\big) * f^{-1}(b),$$
$$f\big(f^{-1}\big(f(a)\big) \circ f^{-1}(b)\big) \neq f\big(f^{-1}\big(f(a)\big) * f^{-1}(b)\big),$$
$$f(a) \circ_f b \neq f(a) *_f b. \qquad \square$$

Proposition 3.2. *Let* $G(\circ)$, $G(*)$ *be groups. Then* $\mathrm{dist}([\circ], [*]) = \mathrm{dist}([\circ], *)$. *Moreover, if* $G(\circ) \cong G(*)$ *then* $\delta(\circ) = \delta(*)$, $\delta_{\cong}(\circ) = \delta_{\cong}(*)$ *and* $\delta_{\ncong}(\circ) = \delta_{\ncong}(*)$.

Proof. Let $f, g : G \to G$ be bijections for which $\mathrm{dist}([\circ], [*]) = \mathrm{dist}(\circ_f, *_g)$. Then, by Lemma 3.1, $\mathrm{dist}([\circ], [*]) = \mathrm{dist}(\circ_f, *_g) = \mathrm{dist}((\circ_f)_{g^{-1}}, *) \geqslant \mathrm{dist}([\circ], *)$. The other inequality is obvious.

Now assume that $* = \circ_f$ for some bijection $f : G \to G$, and let $G(\cdot)$ be such that $\delta(\circ) = \mathrm{dist}(\circ, \cdot)$. Then $\delta(*) \leqslant \mathrm{dist}(*, \cdot_f) = \mathrm{dist}(\circ_f, \cdot_f) = \mathrm{dist}(\circ, \cdot) = \delta(\circ)$, the other inequality follows by symmetry, so $\delta(\circ) = \delta(*)$. The equalities $\delta_{\cong}(\circ) = \delta_{\cong}(*)$ and $\delta_{\ncong}(\circ) = \delta_{\ncong}(*)$ are proved similarly. $\square$

To determine $\mathrm{dist}([\circ], [*])$ it therefore suffices to find the minimal value of $\mathrm{dist}(\circ_f, *)$, where $f : G \to G$ is a bijection.

Let us denote the neutral element of $G(\circ)$ by $1(\circ)$, and the inverse of a in $G(\circ)$ by a°.

Lemma 3.3. *Assume that $G(\circ)$, $G(*)$ have the same neutral element $1(\circ) = 1(*)$, and let $f : G \to G$ be a bijection such that* $\operatorname{dist}([\circ],[*]) = \operatorname{dist}(\circ_f, *)$. *Then either $f(1(\circ)) = 1(\circ)$, or else $\circ_f = *_\ell$ for some transposition ℓ and* $\operatorname{dist}([\circ],[*]) = \operatorname{dist}(*_\ell, *)$.

Proof. Let $G(\cdot) = G(\circ_f)$, so $\operatorname{dist}([\circ],[*]) = \operatorname{dist}(\cdot, *)$. Since $f : G(\circ) \to G(\cdot)$ is an isomorphism, we have $1(\cdot) = f(1(\circ))$. If $1(\cdot) = 1(\circ)$ we are done, so assume that $1(\cdot) = f(1(\circ)) \neq 1(\circ)$. Let $g = \ell \circ f$ be the composition of f with the transposition ℓ of $1(\circ)$ and $1(\cdot)$, and let $G(\bullet) = G(\circ_g)$. We claim that $\operatorname{dist}(\bullet, *) < \operatorname{dist}(\cdot, *)$.

Recall that $1(\circ) = 1(*)$, and consider the set $E = \{(a,b) \in G \times G;\ \{a,b\} \cap \{1(\cdot), 1(*)\} \neq \emptyset\}$. We first show that $G(\cdot)$ and $G(*)$ disagree on every entry of E. Indeed, if $a = 1(\cdot)$ and $b \in G$ then $a \cdot b = 1(\cdot) \cdot b = b = 1(*) * b \neq 1(\cdot) * b = a * b$, if $a = 1(*)$ then $a \cdot b = 1(*) \cdot b \neq 1(\cdot) \cdot b = b = 1(*) * b = a * b$, and similarly if $b \in \{1(\cdot), 1(*)\}$. On the other hand, we claim that $G(\bullet)$ and $G(*)$ agree on the row of E indexed by $1(*)$, and on the column of E indexed by $1(*)$. Indeed, we have $g^{-1}(1(*)) = f^{-1}(1(\cdot)) = 1(\circ)$, and hence $1(*) \bullet b = g(g^{-1}(1(*)) \circ g^{-1}(b)) = g(1(\circ) \circ g^{-1}(b)) = g(g^{-1}(b)) = b = 1(*) * b$, and, similarly, $b \bullet 1(*) = b * 1(*)$. Hence $|E \cap \operatorname{diff}(\cdot, *)| - |E \cap \operatorname{diff}(\bullet, *)| \geqslant 2n - 1$.

Since the operation $\bullet = \circ_g$ is obtained from $\cdot = \circ_f$ by applying the transposition ℓ, the two operations agree outside of E, except possibly on the two "diagonals"

$$F = \big\{(a,b) \in G \times G;\ a \cdot b = 1(*) \text{ or } a \cdot b = 1(\cdot)\big\}.$$

Recall that $1(*) \bullet b = 1(*) * b$ for every $b \in G$, in particular for the two values of b with $(1(*), b) \in F$. Thus, in the worst case, $|F \cap \operatorname{diff}(\cdot, *)| - |F \cap \operatorname{diff}(\bullet, *)| \geqslant 0 - (|F| - 2) = 2 - 2n$. We conclude that $\operatorname{dist}(\bullet, *) < \operatorname{dist}(\cdot, *)$.

This means that $\operatorname{dist}(\bullet, *) = 0$ and thus $\bullet = *$. Since $\bullet = \circ_g = (\circ_f)_\ell$, we see that $\circ_f = *_\ell$. □

While calculating $\operatorname{dist}([\circ],[*])$, we can certainly assume that $1(\circ) = 1(*) = 1$. Lemma 3.3 therefore allows us to consider only mappings f fixing the element 1, or to conclude that $\operatorname{dist}([\circ],[*]) = \operatorname{dist}(*_\ell, *)$ for some transposition ℓ, a case fully resolved by Theorem 1.1 as long as $n \geqslant 5$. This speeds up the search slightly. A much larger improvement is achieved by looking at the automorphism groups of $G(\circ)$ and $G(*)$. Denote by $\operatorname{Aut}(\circ)$ the automorphism group of $G(\circ)$.

Lemma 3.4. *Let $G(\circ)$, $G(*)$ be groups, $f : G \to G$ a bijection, and $g \in \operatorname{Aut}(\circ)$, $\ell \in \operatorname{Aut}(*)$. Then* $\operatorname{dist}(\circ_f, *) = \operatorname{dist}(\circ_{\ell f g}, *)$.

Proof. Note that $\circ_g = \circ$ and $*_\ell = *$. Using these facts and Lemma 3.1, we have $\operatorname{dist}(\circ_f, *) = \operatorname{dist}((\circ_g)_f, *) = \operatorname{dist}(\circ_{fg}, *) = \operatorname{dist}((\circ_{fg})_\ell, *_\ell) = \operatorname{dist}(\circ_{\ell f g}, *_\ell)$. □

4. Structural tools

Recall the parameters (1.2). The results 4.1–4.3 and 4.5–4.9 are taken from [3] and [7], or are immediate corollaries of results therein. We do not hesitate to include short proofs here, and we refer the reader to [3] and [7] for the longer, omitted proofs.

Lemma 4.1. *If $a \circ b \neq a * b$ then* $\operatorname{dist}_a + \operatorname{dist}_b + \operatorname{dist}_{a \circ b} \geqslant n$.

Proof. Let $c \in G$ and suppose that $b \circ c = b * c$ and $(a \circ b) \circ c = (a \circ b) * c$. Then $a \circ (b \circ c) = (a \circ b) \circ c = (a \circ b) * c \neq (a * b) * c = a * (b * c) = a * (b \circ c)$. □

Lemma 4.2. *Let $H = H(\circ, *)$. Then either $H = \emptyset$ or else $H \leqslant G(\circ)$ and $H \leqslant G(*)$.*

Proof. Assume that $a, b \in H$. Then for every $c \in G$ we have $(a \circ b) \circ c = a \circ (b \circ c) = a \circ (b * c) = a * (b * c) = (a * b) * c = (a \circ b) * c$, so $a \circ b \in H$. □

We remark that, as per the previous section, we can always assume that $1 \in H$, so the case when $H = \emptyset$ will not arise in our work.

Lemma 4.3. *Suppose that $H \neq \emptyset$. If $b \in H \circ a$ then $\mathrm{dist}_a = \mathrm{dist}_b$.*

Proof. Let $b = c \circ a$ for $c \in H$. Let $d \in G$ and suppose that $b \circ d = b * d$. Then $c * (a \circ d) = c \circ (a \circ d) = (c \circ a) \circ d = (c \circ a) * d = (c * a) * d = c * (a * d)$, and thus $a \circ d = a * d$. This shows that $\mathrm{dist}_a \leqslant \mathrm{dist}_b$, and the other inequality follows from $a \in H \circ b$. □

Lemma 4.4. *If $a \circ b \neq a * b$ then $H \circ b \neq H \circ (a \circ b)$.*

Proof. If $H \circ b = H \circ (a \circ b)$ then $a = a \circ b \circ b^{\circ} \in H$, contradicting $\mathrm{dist}_a > 0$. □

Lemma 4.5. *If $h(\circ, *) = n/2$ then $\mathrm{dist}(\circ, *) \geqslant n^2/4$.*

Lemma 4.6. *If $h > 0$ then h divides k.*

Proof. Since the function $\mathrm{dist} : G \to \mathbb{N}$, $a \mapsto \mathrm{dist}_a$ takes on different values in K and $G \setminus K$, Lemma 4.3 implies that K is a union of (right) cosets of H. □

Proposition 4.7. *If $k(\circ, *) > 3n/4$ then there is an isomorphism $f : G(\circ) \to G(*)$ fixing all elements of $K(\circ, *)$.*

The following example shows that Proposition 4.7 is best possible. Let $\circ, *$ be defined as follows, where differences are shaded.

$\circ$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	8	7	6	5
4	4	3	2	1	7	8	5	6
5	5	6	8	7	3	4	2	1
6	6	5	7	8	4	3	1	2
7	7	8	6	5	2	1	3	4
8	8	7	5	6	1	2	4	3

$*$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	7	8	3	4	2	1
6	6	5	8	7	4	3	1	2
7	7	8	6	5	2	1	4	3
8	8	7	5	6	1	2	3	4

In this example, $k = 6 = 3n/4$, but the groups are not isomorphic; $G(\circ) \cong C_4 \times C_2$ and $G(*) \cong C_8$.

Proposition 4.8. *Assume that $n \geqslant 12$, and let $f : G(\circ) \to G(*)$ be a nonidentity isomorphism with more than $2n/3$ fixed points. Then $\mathrm{dist}(\circ, *) \geqslant \delta_0(\circ)$.*

Corollary 4.9. *Assume that $n \geqslant 12$. If $k(\circ, *) > 3n/4$ then $G(\circ) \cong G(*)$ and $\mathrm{dist}(\circ, *) \geqslant \delta_0(\circ)$.*

In our search for closest groups $G(*)$ to $G(\circ)$, we can therefore assume that $k \leqslant 3n/4$ when $n \geqslant 12$.

Denote by $L_a(\circ)$ the left translation by a in $G(\circ)$, that is, $L_a(\circ)(b) = a \circ b$. Let $\beta_a(\circ, *) = (L_a(\circ))^{-1} L_a(*)$. Then $\beta_a(\circ, *)(b) = b$ if and only if $a \circ b = a * b$, and thus $\mathrm{dist}_a(\circ, *)$ is the number of points moved by $\beta_a(\circ, *)$.

Lemma 4.10. *Assume that $\mathrm{dist}_a = \mathrm{dist}_a(\circ, *) > 0$. Then $\mathrm{dist}_a \geqslant 2$. If $\beta_a(\circ, *)$ is an even permutation then $\mathrm{dist}_a \geqslant 3$. In particular, if n is odd then $\mathrm{dist}_a \geqslant 3$.*

Proof. The case $\mathrm{dist}_a = 1$ is impossible since β_a cannot move precisely 1 point. When β_a is even, it is not a transposition, and hence it moves at least 3 points. When n is odd, the left translations $L_a(\circ)$, $L_a(*)$ are products of cycles of odd length, hence β_a is an even permutation. □

Finally, we investigate $\operatorname{dist}_a(\circ,*)$ depending on whether a has the same order in $G(\circ)$ and $G(*)$. Denote by $|a|_\circ$ the order of a in $G(\circ)$. If $|a|_\circ = |a|_*$, we say that a is *order matched*, otherwise it is *order mismatched*.

Lemma 4.11. *Assume that* $\sigma = |a|_\circ > |a|_* = \tau$. *Then* $\operatorname{dist}_a(\circ,*) \geqslant (n/\sigma)\lceil \sigma/\tau \rceil \geqslant n/\tau$.

Proof. The left translation $L_a(\circ)$ is a product of n/σ disjoint cycles of length σ, and $L_a(*)$ is a product of n/τ disjoint cycles of length $\tau < \sigma$. Consider a cycle $(b_0,\dots,b_{\sigma-1})$ of $L_a(\circ)$. By definition then, $a \circ b_i = b_{i+1 \bmod \sigma}$. Let us focus on b_0. Without loss of generality, there is a cycle $(c_0,\dots,c_{\tau-1})$ of $L_a(*)$ such that $b_0 = c_0$. Let i be the least integer with $1 \leqslant i \leqslant \tau$ such that $b_i \neq c_{i \bmod \tau}$. (Such an i exists, since $c_{\tau \bmod \tau} = c_0 = b_0 \neq b_\tau$.) Then $a \circ c_{i-1} = a \circ b_{i-1} = b_i \neq c_{i \bmod \tau} = a * c_{i-1} = a * b_{i-1}$.

Hence, corresponding to the segment $b_0,\dots,b_\tau$, we found a difference $a \circ b_j \neq a * b_j$ with $0 \leqslant j \leqslant \tau - 1$. Repeating this argument shows that there must be $\lceil \sigma/\tau \rceil$ differences within each of the n/σ cycles of $L_a(\circ)$. □

By Theorem 1.1, $\delta_{\cong}(\circ) < \delta_{\ncong}(\circ)$ when $n \geqslant 51$. We can reach the same conclusion for some smaller orders n, too:

Lemma 4.12. *Let* $n = 2p$ *for a prime* $p \geqslant 11$. *Let* $G(\circ)$ *be a group of order* n. *Then* $\delta_{\cong}(\circ) < \delta_{\ncong}(\circ)$.

Proof. Up to isomorphism, there are only two groups of order $2p$, the cyclic group $C_{2p} = G(\circ)$ and the dihedral group $D_{2p} = G(*)$. There is a unique involution in C_{2p} and there are p involutions in D_{2p}. Hence at least $p-1$ involutions are order mismatched. By Lemma 4.11, $d_a(\circ,*) \geqslant 2p/2 = p$ for every order mismatched involution a. We therefore have $\operatorname{dist}(\circ,*) \geqslant (p-1)p$. On the other hand, $\delta(C_{2p}) \leqslant 12p - 24$ and $\delta(D_{2p}) \leqslant 12p - 20$ by Theorem 1.1. The inequality $(p-1)p > 12p - 20$ holds for every $p \geqslant 13$.

It remains to discuss the case $p = 11$. If at least one element a in the cyclic subgroup C_p of D_{2p} satisfies $\operatorname{dist}_a > 0$ (hence $\operatorname{dist}_a \geqslant 2$), then the same inequality holds for every nonidentity element of C_p, by Lemma 4.2, and thus $\operatorname{dist}(\circ,*) \geqslant (p-1)p + 2(p-1) > 12p - 20$. Otherwise, $C_p = H$, and $\operatorname{dist}(\circ,*) \geqslant 2p^2 > 12p - 20$ by Lemma 4.5. □

Lemma 4.13. *If* $\operatorname{dist}_a > 0$ *and* a *is order matched then* $\operatorname{dist}_a \geqslant 3$.

Proof. The two left translations $L_a(\circ)$ and $L_a(*)$ have the same cycle structure, thus $\beta_a(\circ,*)$ is an even permutation, and we are done by Lemma 4.10. □

We can now narrow down possible isomorphism types of $G(\circ)$ and $G(*)$ when $m = 2$.

Proposition 4.14. *Assume that* $\operatorname{dist}_a(\circ,*) = 2$. *Then, without loss of generality,* $|a|_\circ = n$ *and* $|a|_* = n/2$.

Proof. Since $\operatorname{dist}_a = 2$, a must be order mismatched, by Lemma 4.13. Let $\sigma = |a|_\circ$ and $\tau = |a|_*$. Without loss of generality, $\sigma > \tau$. Then, by Lemma 4.11, $2 = \operatorname{dist}_a \geqslant (n/\sigma)\lceil \sigma/\tau \rceil$. As $\sigma > \tau$, we must have $n/\sigma = 1$ and $\lceil \sigma/\tau \rceil = 2$, hence $n = \sigma$, $\lceil n/\tau \rceil = 2$, and because τ divides n, it follows that $\tau = n/2$. □

For a group $G(\circ)$ and integer $\ell \geqslant 1$, let $o_\ell(\circ)$ be the number of elements of order ℓ in $G(\circ)$. Motivated by Proposition 4.14, we let

$$\omega(\circ,*) = \min\bigl\{o_n(\circ), o_{n/2}(*)\bigr\} + \min\bigl\{o_{n/2}(\circ), o_n(*)\bigr\}.$$

Let φ denote Euler's totient function.

Lemma 4.15. *For groups $G(\circ)$, $G(*)$ of even order n, there are at most $h(\circ,*)+2\varphi(n/2)$ rows $a\in G$ with* $\operatorname{dist}_a<3$.

Proof. Consider $a\notin H$. If a is order matched, then $\operatorname{dist}_a\geqslant 3$ by Lemma 4.13. If a is order mismatched and $\operatorname{dist}_a=2$, we must have $\{|a|_\circ,|a|_*\}=\{n,n/2\}$, by Lemma 4.11. The number of elements a with $\{|a|_\circ,|a|_*\}=\{n,n/2\}$ cannot exceed $\omega(\circ,*)$. Thus it suffices to show that $\omega(\circ,*)\leqslant 2\varphi(n/2)$.

Suppose $G(\circ)$ is not cyclic. Then $\omega(\circ,*)=\min\{0,o_{n/2}(*)\}+\min\{o_{n/2}(\circ),o_n(*)\}\leqslant o_n(*)\leqslant\varphi(n)\leqslant 2\varphi(n/2)$. A similar argument works if $G(*)$ is not cyclic, so we may as well assume that both $G(\circ)$ and $G(*)$ are cyclic. In that case $\omega(\circ,*)=2\min\{o_{n/2}(\circ),o_n(*)\}=2\min\{\varphi(n/2),\varphi(n)\}=2\varphi(n/2)$. □

5. Inequalities

We now start the search for closest multiplication tables of groups.

Let $G(\circ)$, $G(*)$ be two groups of order n, and let $h=h(\circ,*)$, $k=k(\circ,*)$, $m=m(\circ,*)$. Keeping our goal in mind, we can make the following assumptions on n, h, k and m:

- $23\leqslant n\leqslant 50$ (the case $n\geqslant 51$ is covered by Theorem 1.1, the case $n\leqslant 22$ will be addressed later),
- $1\leqslant h<n$ and h divides n (we can assume $1\leqslant h$ by Lemma 3.3, $h<n$ to avoid $G(\circ)=G(*)$, and h divides n by Lemma 4.2),
- $k\leqslant 3n/4$ and h divides k (by Corollary 4.9 and Lemma 4.6),
- $m\geqslant 2$ when n is even and $m\geqslant 3$ when n is odd (by Lemma 4.10). By the definition of k, we also know $m<n/3$ if $h<k$, whereas $n/3\leqslant m\leqslant n$ if $h=k$.

We will consider quadruples (n,h,k,m) satisfying the above conditions. We are interested only in such quadruples for which $\operatorname{dist}(\circ,*)\leqslant\delta(\circ)$ occurs. Since we do not want to assume (yet) anything about the isomorphism type of $G(\circ)$, we set

$$\delta_0(n)=\begin{cases}6n-18, & \text{when } n \text{ is odd},\\ 6n-20, & \text{when } n\equiv 2 \bmod 4,\\ 6n-24, & \text{when } n\equiv 0 \bmod 4,\end{cases}$$

and we keep only those quadruples for which it is possible that $\operatorname{dist}(\circ,*)\leqslant\delta_0(n)$. We will eliminate most quadruples by a series of inequalities.

We start with a fundamental inequality based on both H and K. Every element of $G\setminus K$ satisfies $\operatorname{dist}_a\geqslant\lceil n/3\rceil$, and $H\subseteq K$, thus

$$\operatorname{dist}(\circ,*)\geqslant(n-k)\lceil n/3\rceil+(k-h)m. \tag{5.1}$$

There are 309 quadruples $[n,h,k,m]$ that satisfy this constraint. We will gradually whittle these away until none remain (at the end of Section 10).

Let a be such that $\operatorname{dist}_a=m$. By Lemma 4.1, there is b such that $\operatorname{dist}_a+\operatorname{dist}_b+\operatorname{dist}_{a\circ b}\geqslant n$. Hence $\operatorname{dist}_b+\operatorname{dist}_{a\circ b}\geqslant n-m$, and we conclude that there exists c such that $\operatorname{dist}_c\geqslant\lceil(n-m)/2\rceil$. Then by Lemma 4.3, there are (at least) h elements c with $\operatorname{dist}_c\geqslant\lceil(n-m)/2\rceil$, all in $G\setminus H$. The remaining $n-2h\geqslant 0$ elements of $G\setminus H$ satisfy $\operatorname{dist}_a\geqslant m$, and we have

$$\operatorname{dist}(\circ,*)\geqslant h\left\lceil\frac{n-m}{2}\right\rceil+(n-2h)m. \tag{5.2}$$

(282 quadruples remain.)

By Lemma 4.5,

$$\text{if } h=n/2 \quad \text{then } \operatorname{dist}(\circ,*)\geqslant n^2/4. \tag{5.3}$$

(207 quadruples remain, all with $m<n/3$ and $h<k$.)

Let again $a \circ b \neq a * b$, and assume $\mathrm{dist}_a = m$. Then $\mathrm{dist}_b + \mathrm{dist}_{a\circ b} \geqslant n - m$. By Lemma 4.4, the cosets $H \circ b$ and $H \circ (a \circ b)$ are distinct. Since dist_c is constant within every right coset of H by Lemma 4.3, there are $2h$ elements with average value of dist_c at least $(n-m)/2$. On one of these 2 cosets, $\mathrm{dist}_c \geqslant (n-m)/2$, which puts this coset into $G \setminus K$, as $(n-m)/2 > n/3$ (using $m < n/3$). If we temporarily assume that $n - k < 2h$, the second coset cannot be located in $G \setminus K$, so we have

$$\text{if } n-k<2h \quad \text{then } \mathrm{dist}(\circ,*) \geqslant h(n-m) + (n-k-h)\lceil n/3\rceil + (k-2h)m. \tag{5.4}$$

(188 quadruples remain, all with $n - k \geqslant 2h$.)

Returning to the two cosets with average value of dist_c at least $(n-m)/2$, even if both are located within $G \setminus K$, we at least have

$$\mathrm{dist}(\circ,*) \geqslant h(n-m) + (n-k-2h)\lceil n/3\rceil + (k-h)m. \tag{5.5}$$

(99 quadruples remain.)

In the previous inequality, we have used $\mathrm{dist}_a > m$ on $n - k$ rows. If $m = 2$, there are at most $h + 2\varphi(n/2)$ rows with $\mathrm{dist}_a = 2$, by Lemma 4.15, so there are at least $n - (h + 2\varphi(n/2)) - (n-k) = k - h - 2\varphi(n/2)$ rows where we used $\mathrm{dist}_a = 2$ in (5.5) but could have used $\mathrm{dist}_a \geqslant 3$. This number of rows might be negative, but we certainly have

$$\text{if } m=2 \quad \text{then } \mathrm{dist}(\circ,*) \geqslant h(n-m) + (n-k-2h)\lceil n/3\rceil + (k-h)m + k - h - 2\varphi(n/2). \tag{5.6}$$

(89 quadruples remain.)

Finally, we eliminate the case $n = 32$:

Lemma 5.1. *(See [6, Lemma 4.4].) Let $G(\circ)$, $G(*)$ be isomorphic 2-groups of order n satisfying $\mathrm{dist}(\circ,*) < n^2/4$. Then there exists a bijection $f : G \to G$ with at least $(n/4)(3 + 1/\sqrt{3})$ fixed points and such that $* = \circ_f$.*

Corollary 5.2. *Let $G(\circ)$ be a group of order 32. Then $\delta_{\not\cong}(\circ) > \delta_{\cong}(\circ) = \delta_0(\circ) = 168$, and there is a transposition $g : G \to G$ such that $\delta(\circ) = \mathrm{dist}(\circ, \circ_g)$.*

Proof. Let $n = 32$. Recalling the results from the Introduction, we know that $\delta_{\not\cong}(\circ) \geqslant n^2/4 > \delta_0(\circ) = 6 \cdot 32 - 24 = 168$. Let $G(*) \cong G(\circ)$ be such that $\delta(\circ) = \mathrm{dist}(\circ,*)$. Since $\delta(\circ) < n^2/4$, Lemma 5.1 yields a bijection $f : G \to G$ with at least $(n/4)(3 + 1/\sqrt{3}) > 2n/3$ fixed points. By Proposition 4.8, $\mathrm{dist}(\circ,*) \geqslant \delta_0(\circ)$. We are done by Theorem 1.1. □

The remaining 82 quadruples (n, h, k, m) are as follows (quadruples with the same n, h, m are grouped):

$(23, 1, \{13, 14, 15, 16, 17\}, 3)$, $(23, 1, \{16, 17\}, 4)$, $(24, 1, \{14, 15, 16, 17, 18\}, 2)$,
$(24, 1, \{15, 16, 17, 18\}, 3)$, $(24, 1, 18, 4)$, $(24, 2, \{14, 16, 18\}, 2)$,
$(24, 2, \{16, 18\}, 3)$, $(24, 2, 18, 4)$, $(24, 3, \{15, 18\}, 2)$,
$(24, 3, 18, 3)$, $(24, 3, 18, 4)$, $(24, 4, 16, 2)$,
$(24, 4, 16, 3)$, $(25, 1, \{16, 17, 18\}, 3)$, $(26, 1, \{15, 16, 17, 18, 19\}, 2)$,
$(26, 1, \{17, 18, 19\}, 3)$, $(26, 2, \{16, 18\}, 2)$, $(26, 2, 18, 3)$,
$(27, 1, \{17, 18, 19, 20\}, 3)$, $(27, 1, 20, 4)$, $(27, 3, 18, 3)$,

$$
\begin{array}{lll}
(28,1,\{19,20,21\},2), & (28,1,\{20,21\},3), & (28,2,20,2),\\
(28,2,20,3), & (28,4,20,2), & (29,1,\{20,21\},3),\\
(30,1,\{19,20,21,22\},2), & (30,1,\{21,22\},3), & (30,2,\{20,22\},2),\\
(30,2,22,3), & (30,3,21,2), & (31,1,\{22,23\},3),\\
(33,1,24,3), & (34,1,\{23,24,25\},2), & (34,2,24,2),\\
(35,1,26,3), & (36,1,27,2), & (38,1,\{27,28\},2),\\
(38,2,28,2), & (42,1,31,2). &
\end{array}
\tag{5.7}
$$

6. Special row differences

6.1. The case $m = 2$

In this subsection we describe an algorithm that determines all pairs of groups $G(\circ)$, $G(*)$ with $m(\circ,*) = 2$.

By Proposition 4.14, we can assume that $G(*)$ is a fixed cyclic group of even order n, and there is $a \in G$ such that $|a|_* = n$, $|a|_\circ = n/2$.

The automorphism group $\mathrm{Aut}(C_n)$ acts transitively on the generators of C_n. Thus, if b is a generator of $G(*)$, there is $f \in \mathrm{Aut}(*)$ such that $f(a) = b$. By Lemma 3.1, we then have $\mathrm{dist}_a(\circ,*) = \mathrm{dist}_{f(a)}(\circ_f,*_f) = \mathrm{dist}_b(\circ_f,*)$ and $\mathrm{dist}(\circ,*) = \mathrm{dist}(\circ_f,*)$. We can therefore assume without loss of generality that a is a fixed generator of $G(*)$.

The input of the algorithm is a cyclic group $G(*) = C_n$ and its generator a. To obtain $\mathrm{dist}_a(*,\circ) = 2$, we must modify the row a of $G(*)$ in two places; say there are $v \neq w$ such that $a \circ b = a * b$ except for $a \circ v = a * w$, $a \circ w = a * v$. Since $a \circ b$ is now determined for every $b \in G$, we can see if $|a|_\circ = n/2$, as desired. If not, we choose different v, w.

Assume now that the locations v, w of differences in row a were chosen so that $|a|_\circ = n/2$. Let A be the subgroup generated by a in $G(\circ)$, and let b be any element of $G \setminus A$. Denote by a^i the ith power of a in $G(\circ)$. Since $G = A \cup (A \circ b) = A \cup (b \circ A)$, we must have $b \circ a = a^\alpha \circ b$ for some $1 \leqslant \alpha < n/2$, and $b \circ b = a^\beta$ for some $0 \leqslant \beta < n/2$. Once the parameters α, β are chosen, the operation $\circ$ is determined, namely:

$$
\begin{aligned}
a^i \circ a^j &= a^{i+j},\\
a^i \circ \left(a^j \circ b\right) &= a^{i+j} \circ b,\\
\left(a^i \circ b\right) \circ a^j &= a^i \circ \left(b \circ a^j\right) = a^i \circ \left(a^{j\alpha} \circ b\right) = a^{i+j\alpha} \circ b,\\
\left(a^i \circ b\right) \circ \left(a^j \circ b\right) &= a^i \circ \left(b \circ a^j\right) \circ b = a^{i+j\alpha} \circ b \circ b = a^{i+j\alpha+\beta},
\end{aligned}
$$

for $0 \leqslant i, j < n/2$. We do not claim that this operation defines a group, only that there is no alternative way to define $\circ$ that does produce a group (as it happens, the smallest distance is achieved when $\circ$ does define a group).

It therefore suffices to consider all choices of v, w, α, β and find the resulting groups closest to $G(*)$. Both authors independently ran this algorithm and discovered that in all cases the nearest group $G(\circ)$ was isomorphic to $C_{n/2} \times C_2$ and satisfied

$$
\mathrm{dist}(\circ,*) = \begin{cases} n^2/4, & \text{when } n \equiv 0 \bmod 4,\\ n^2/4 - 1, & \text{when } n \equiv 2 \bmod 4. \end{cases}
$$

Since $n^2/4 - 1 > \delta_0(n)$ when $n > 20$, the quadruples of (5.7) with $m = 2$ can therefore be eliminated. (43 quadruples remain.)

6.2. Some cyclic cases

Among the remaining orders n of (5.7), if n belongs to $\{23, 29, 31, 33, 35\}$, the only group of order n is the cyclic group C_n. For these orders, the search therefore amounts to determination of $\operatorname{dist}([C_n], [C_n])$, a difficult task in general.

Let $G(\circ)$ be a cyclic group of order n. For any group $G(*)$, define

$$m' = m'(\circ, *) = \min\bigl\{\operatorname{dist}_a(\circ, *);\ |a|_\circ = n\bigr\}.$$

Recall that C_n has $\varphi(n)$ generators. Since m' might be bigger than m, we can refine (5.5) as follows,

$$\operatorname{dist}(\circ, *) \geqslant h(n-m) + (n-k-2h)\lceil n/3\rceil + \bigl(\varphi(n) - (n-k)\bigr)m' + \bigl(n - \varphi(n) - h\bigr)m, \qquad (6.1)$$

where we first count elements in the two cosets of H, then all remaining elements of $G \setminus K$, then all remaining generators, and then the remaining elements in $G \setminus H$, if any.

To eliminate all remaining quadruples with $n \in \{29, 31, 33, 35\}$ (resp. $n = 23$), it suffices to set $m' = 4$ (resp. $m' = 5$) in (6.1).

We are therefore interested in the following algorithm, with parameter d: Given $G(\circ) \cong C_n$, find $G(\circ) \cong C_n$ closest to $G(*)$ that has $\operatorname{dist}_a(\circ, *) = d$ for some generator a of $G(\circ)$.

The idea is similar to Section 6.1, but we reverse the roles of the groups $G(\circ)$ and $G(*)$. Let $a \in G$ be such that $|a|_* = \ell$. We wish to have $|a|_\circ = n$ and $\operatorname{dist}_a(\circ, *) = m'$. By Lemma 4.11, we can assume that $n/\ell \leqslant d$ (since $|a|_\circ = n$), that is, $\ell \geqslant n/d$.

Let us fix $a \in G$ with the above properties. We now need to make d changes to row a of $G(*)$, focusing on only those changes that result in $|a|_\circ = n$. Once such a change is made, the group $G(\circ)$ is determined.

Remark 6.1. When n is a prime, the search can be sped up by taking advantage of the automorphism group of C_n (since all nonidentity elements are generators), and by analyzing which permutations of $\operatorname{diff}_a(\circ, *)$ result in $|a|_\circ = n$. See [17] or [18] for details. We did not employ these improvements here in order to keep the code simpler.

For every quadruple (n, h, k, m) of (5.7) with $n \in \{23, 29, 31, 33, 35\}$, the algorithm (with $d = 3$ if $n \in \{29, 31, 33, 35\}$ and with $d \in \{3, 4\}$ if $n = 23$) returns minimal distance at least as big as $\delta_0(n)$. (30 quadruples remain.)

7. General algorithm for dist([∘], [∗])

Here is an algorithm that finds $d = \operatorname{dist}([\circ], [*])$. By Proposition 3.2, we have $d = \operatorname{dist}([\circ], *) = \min\{\operatorname{dist}(\circ_f, *);\ f : G \to G \text{ is a bijection, } G(\circ_f) \neq G(*)\}$.

When $n < 5$ a brute force algorithm is sufficient. Let us therefore assume that $n \geqslant 5$ and, by Lemma 3.3, that $f(1) = 1$ and thus $1 \in H$.

Either $H = 1$ or there exists a prime p and a subgroup $\overline{H} \leqslant H$ of $G(*)$ of order p. The main cycle of the algorithm proceeds over all subgroups $\overline{H} \leqslant G(*)$ of prime order p or $p = 1$, with $|\overline{H}|$ in descending order. From now on we will write H instead of $\overline{H}$, since the fact that H might be larger is irrelevant in the search.

Assume that $\operatorname{dist}_{min}$ is the smallest distance found by the algorithm so far, and let $H \leqslant G(*)$, $|H| = p$ be given. We need to consider all bijections $f : G \to G$ such that $G(\cdot) = G(\circ_{f^{-1}})$ and $G(\circ)$ agree on at least H. The inverse f^{-1}, rather than f, is used for notational convenience, and we then have $f(a \cdot b) = f(a) \circ f(b)$.

The algorithm is a depth-first search on all partially defined 1-to-1 maps $f : G \to G$, where the maps are lexicographically ordered as follows: Let $\operatorname{Dom}(f)$ denote the domain of f, and let $G =$

$\{1,\dots,n\}$. Let $f, g : G \to G$ be two partially defined maps. Then we say that $g < f$ if and only if there exists $i \in \mathrm{Dom}(f)$ such that (a) for every $j \leqslant i$, if $j \in \mathrm{Dom}(f)$ then $j \in \mathrm{Dom}(g)$, (b) for every $j < i$, if $j \in \mathrm{Dom}(f)$ then $g(j) = f(j)$, (c) $g(i) < f(i)$.

The search starts as follows: Let x be a generator of H. Then $f(x)$ is an element of order p in $G(\circ)$, because we demand that $x \in H(\cdot,*) = H$ and that $f : G(\cdot) \to G(\circ)$ is an isomorphism. The second cycle of the algorithm is therefore over all elements $y = f(x)$ such that $|y|_\circ = p$.

Once $f(x)$ is known, we can extend f onto H. Indeed, we have $f(x*x) = f(x\cdot x)$ by our assumption that $H = H(\cdot,*)$, and $f(x\cdot x) = f(x)\circ f(x)$ because $f : G(\cdot) \to G(\circ)$ is a homomorphism. Similarly for higher powers of x.

To extend the domain of f further, we systematically choose $b \notin \mathrm{Dom}(f)$, $c \notin \mathrm{Im}(f)$, and declare $f(b) = c$. Once again, we can now extend f onto the coset $H*b$, as for $y \in H$ we must have $f(y*b) = f(y\cdot b) = f(y)\circ f(b)$.

Anytime we extend the domain of f by another coset of H, we can calculate the guaranteed distance between the partially defined group $G(\cdot)$ and the group $G(*)$ by counting only those pairs (a,b) that satisfy: $a \in \mathrm{Dom}(f)$, $b \in \mathrm{Dom}(f)$, $a\cdot b \in \mathrm{Dom}(f)$ and $f(a\cdot b) \neq f(a)\circ f(b)$. If this distance exceeds dist_{min}, we terminate this branch of the depth-first search.

Whenever we extend the domain of f by another coset, we consider the automorphisms $g \in \mathrm{Aut}(\circ)$ and $\ell \in \mathrm{Aut}(*)$. By Lemma 3.4, $\mathrm{dist}(\circ_{\ell fg},*) = \mathrm{dist}(\circ_f,*)$. It is also easy to see that $H(\circ_{\ell fg},*) = H(\circ_f,*)$. Therefore, if $\ell fg < f$, we have seen ℓfg before f (in this cycle with the same H), f cannot do better than ℓfg as far as distance is concerned, so we terminate the branch.

If $\mathrm{Dom}(f) = G$ anytime in the search, we calculate the full distance $\mathrm{dist}(\cdot,*)$ and compare it to dist_{min}.

The following improvements make the algorithm faster:

- the distance $\mathrm{dist}(\cdot,*)$ is calculated incrementally, in every step considering only rows, columns and values from the coset of H on which f has just been defined,
- the comparison of ℓfg to f is costly, and it is better to stop using it in the search from a certain (heuristically determined) depth in the search,
- assuming that the algorithm has gone through all values of $p > 1$ and is now in the cycle $p = 1$, the guaranteed distance can be calculated with a bonus. Namely, since we have $H = 1$ at this stage, we can assume that every row not in the domain of f contains 2 (resp. 3) differences when n is even (resp. odd), by Lemma 4.10.

The algorithm is sufficiently fast to deal with all orders $n \leqslant 22$, albeit in some cases we merely verified that $\mathrm{dist}([\circ],[*])$ exceeds $\delta(\circ)$, without actually determining $\mathrm{dist}([\circ],[*])$. The case $n = 22$ alone took more than a week of computing time. It was therefore of some importance that we could assume $G(\circ) \cong G(*)$ when $n = 22$, by Lemma 4.12.

The results of the search for $n \leqslant 22$ are summarized in Theorem 2.1.

The algorithm can also be used to eliminate all remaining cases of (5.7) with $h > 1$; we simply do not run the algorithm with any values p less than h. This leaves us with the following twenty quadruples (n,h,k,m):

$$\begin{array}{lll} \big(24,1,\{15,16,17,18\},3\big), & (24,1,18,4), & \big(25,1,\{16,17,18\},3\big) \\ \big(26,1,\{17,18,19\},3\big), & \big(27,1,\{17,18,19,20\},3\big), & (27,1,20,4) \\ \big(28,1,\{20,21\},3\big), & \big(30,1,\{21,22\},3\big). & \end{array} \tag{7.1}$$

We eliminate them in Section 10, but first we need to introduce results on rainbow matchings in edge-colored graphs.

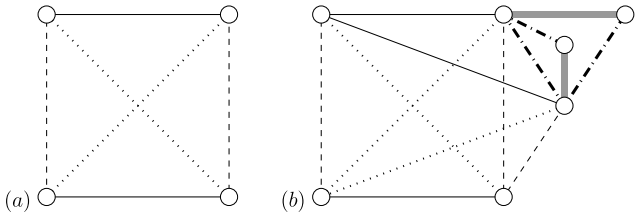

Fig. 1. Restricted graphs giving lower bounds for Proposition 8.1.

8. Rainbow matchings and the graph Γ_U

Call an edge-colored graph *restricted* if it has at most 3 edges of any given color, and if at most two edges of the same color are incident at any vertex. Recall that a *rainbow ℓ-matching* in an edge-colored graph is a set of ℓ disjoint edges colored by distinct colors. For $v > 1$ and $\ell > 0$, define $\mu_\ell(v)$ to be the minimum number of edges a restricted graph on v vertices must have in order to guarantee a rainbow ℓ-matching. If there exists a coloring of the complete graph on v vertices that yields a restricted graph without a rainbow ℓ-matching, then we define $\mu_\ell(v) = \binom{v}{2} + 1$.

Proposition 8.1. *We have $\mu_1(v) = 1$ for every $v \geqslant 2$, $\mu_2(v) = 7$ if $4 \leqslant v \leqslant 6$, $\mu_2(v) = v$ if $v \geqslant 7$, $\mu_3(6) = 13$, $\mu_3(7) = 15$, $\mu_3(8) = 15$, $\mu_3(9) = 16$ and $\mu_3(10) = 18$.*

We now describe the algorithm used to establish Proposition 8.1. The aim was to find the greatest number of edges that a restricted graph on v vertices can have without containing a rainbow ℓ-matching. We began with an empty graph on v vertices, and added the edges one color at a time. We will refer to the process of adding all the edges of a particular color as a *stage*. In each stage, we read in each of the graphs from the previous stage, one at a time, added edges of the new color in all possible ways, and output any graph which was not isomorphic (by an isomorphism that respects the edge coloring, but is allowed to permute colors) to a graph we had already seen. The isomorphism testing was accomplished by `nauty` [14].

After a graph was read in stage c, we found all rainbow $(\ell - 1)$-matchings in it. Any edge disjoint from any such matching is unavailable to be colored c. Typically this rule leaves very few edges still available. We also sped up the search by making several other assumptions. Firstly, since all isolated vertices are isomorphic, vertex $j + 1$ would not be connected to its first edge before vertex j was. Secondly, for $c > 1$ we insisted that there were not more edges of color c than there were of color $c - 1$. Thirdly, we assumed that there was at most one color which occurs on only one edge. This last assumption is justified because if two colors each only occurred on one edge then we could replace those two colors by a single color. The result would still be a restricted graph, and would not have a rainbow ℓ-matching unless the original graph did.

As a partial validation of our computations, it is easy to confirm by hand that the values quoted in Proposition 8.1 are lower bounds on $\mu_\ell(v)$. First note that we can prevent a rainbow ℓ-matching by having no ℓ-matchings at all. This can be achieved by having a set of $\ell - 1$ vertices that cover all edges, in which case we can have up to $\binom{\ell-1}{2} + (\ell - 1)(v - \ell + 1) = (\ell - 1)(v - \ell/2)$ edges. Thus $\mu_\ell(v) \geqslant 1 + (\ell - 1)(v - \ell/2)$ whenever $v \geqslant \ell - 1$. This elementary lower bound is actually achieved for $\mu_1(v)$, $v \geqslant 1$; $\mu_2(v)$, $v \geqslant 7$; and $\mu_3(v)$, $v \in \{9, 10\}$. To give a lower bound for the other values quoted in Proposition 8.1, we display in Fig. 1 graphs with (a) 4 vertices, 6 edges and no rainbow 2-matching, (b) 7 vertices, 14 edges and no rainbow 3-matching. Edge colors are indicated by the different styles of lines. By deleting either of the degree 2 vertices from (b) we obtain a graph with 6 vertices, 12 edges and no rainbow 3-matching. These examples show that $\mu_2(v) \geqslant 7$ for $v \geqslant 4$, $\mu_3(6) \geqslant 13$ and $\mu_3(8) \geqslant \mu_3(7) \geqslant 15$.

The statement in Proposition 8.1 that $\mu_2(v) = v$ for $v \geqslant 7$ is easily seen. We have already argued that $\mu_2(v) \geqslant v$. Suppose we have a restricted graph with $v \geqslant 7$ vertices and v edges and no rainbow 2-matching. Any graph with $v > 3$ vertices and v edges has a 2-matching; in our case both edges

must have the same color c. Every edge of color different from c must join the two edges of the 2-matching, and there are only 4 possible places to put such an edge. There may be a third edge of color c, but that is all. Thus our graph has at most 7 edges. The case $v = e = 7$ can be handled by more detailed case analysis, or ruled out by our computer programs.

Let us now return to the problem of distances of groups. The following subsets of $\mathrm{diff}(\circ, *)$ will play an important role in the analysis of the cases (7.1). Let

$$\begin{aligned}
R = R(\circ,*) &= \big\{(a,a) \in \mathrm{diff}(\circ,*);\ a \in K\big\}, \qquad r = r(\circ,*) = |R|,\\
S = S(\circ,*) &= \big\{(a,b) \in \mathrm{diff}(\circ,*);\ a \in K,\ b \in K,\ a \neq b\big\}, \qquad s = s(\circ,*) = |S|,\\
T = T(\circ,*) &= \big\{(a,b) \in \mathrm{diff}(\circ,*);\ a \in K,\ a \circ b \in K\big\}, \qquad t = t(\circ,*) = |T|,\\
U' = U'(\circ,*) &= \big\{(a,b) \in \mathrm{diff}(\circ,*);\ a \in K,\ a \circ b \notin K,\ b \notin K\big\}.
\end{aligned} \tag{8.1}$$

Note that, R, S, T, U' are disjoint and $R \cup S \cup T \cup U' = \mathrm{diff}(\circ, *) \cap (K \times G)$, a set that contains at least $m \geqslant 3$ elements in every row indexed by $K \setminus H$. Let U be any minimal subset of U' subject to the condition that $R \cup S \cup T \cup U$ contains at least 3 elements within each row indexed by $K \setminus H$. Let $u = u(\circ, *) = |U|$. We have

$$r + s + t + u \geqslant 3(k - h). \tag{8.2}$$

Note that if $(a, b) \in S(\circ, *)$, then we must have $a \circ b \notin K$ (and $a * b \notin K$), since otherwise $\mathrm{dist}_a + \mathrm{dist}_b + \mathrm{dist}_{a\circ b} < n$ (and $\mathrm{dist}_a + \mathrm{dist}_b + \mathrm{dist}_{a*b} < n$), a contradiction of Lemma 4.1. Similarly, if $(a, b) \in T(\circ, *)$ then $b \notin K$.

Define a multigraph Γ'_U on vertices $V = G \setminus K$ by declaring $\{x, y\} \subseteq V$ to be an edge if and only if $x \neq y$ and $\{x, y\} = \{b, a \circ b\}$ for some $(a, b) \in U$. Such an edge $\{x, y\} = \{b, a \circ b\}$ will be colored a.

If $\{x, y\} = \{b, a \circ b\} = \{d, c \circ d\}$ is an edge of Γ'_U for some $(a, b), (c, d) \in U$, one of the following situations occurs. If $b = d$ then $a \circ b = c \circ b$, $a = c$, and $(a, c) = (b, d)$. Otherwise $b = c \circ d$, $d = a \circ b$, $a \circ c \circ d = d$, and $c = a^\circ$. Therefore Γ'_U has at most two edges between any two given vertices. If two distinct edges colored a are incident to a vertex of Γ'_U, they are of the form $\{b, a \circ b\}$, $\{c, a \circ c\}$ for some $b \neq c$. Then, without loss of generality, we have $b = a \circ c$. This means that no more than two distinct edges colored a are incident to a vertex of Γ'_U.

Let Γ_U be the simple subgraph of Γ'_U obtained by suppressing any multiple edges. By construction, Γ_U is a restricted graph on $n - k$ vertices. Moreover, any edge of Γ_U colored a stems from some element $(a, b) \in U$. Later we will use (8.2) to find a lower bound for u. In creating Γ_U from Γ'_U, there are at least $\lceil u/2 \rceil$ edges that remain. Having built a restricted graph with at least a certain number of edges, we will be in a position to employ Proposition 8.1.

9. Eliminating cases with a rainbow 3-matching in Γ_U

For the rest of this section, fix $G(\circ)$, $G(*)$, assume that $m(\circ, *) \geqslant 3$, let $q = \lceil n/3 \rceil$, and let

$$\pi = \mathrm{dist}(\circ, *) - \big((k - h)m + (n - k)q\big)$$

be the number of differences above those guaranteed by the fundamental inequality (5.1). We will refer to π as the *profit*. If we wish to indicate the profit obtained in particular rows $r_1, \ldots, r_\ell$, we use the notation $\pi(r_1, \ldots, r_\ell)$.

We present a series of lemmas that eliminate most quadruples of (7.1). While attempting to eliminate a quadruple (n, h, k, m) from (7.1), we proceed as follows: We use Lemmas 9.1, 9.2 and, if $n = 2p$, also Lemma 9.3, to obtain an upper bound on r, with default bound $r \leqslant k - h$. Lemmas 9.4 and 9.6 yield an upper bound on s, with default bound $s \leqslant (k - 1)(k - h)$. The dual Lemmas 9.7 and 9.9 yield an upper bound on t, with default bound $t \leqslant (n - k)(k - h)$. Then (8.2) provides a lower bound for u.

Recall that there are $n-k$ vertices and at least $\lceil u/2\rceil$ edges in Γ_U. We then use Proposition 8.1 to determine the maximal ℓ such that $\lceil u/2\rceil \geqslant \mu_\ell(n-k)$. Finally, we apply Lemma 9.10, and if this yields a sufficient profit then (n,k,h,m) is eliminated.

The challenge is not to count profit on the same row more than once. We often use the following *disjunction tricks* to make sure that this does not happen. If $(a,a)\in R$ then we have $2\,\mathrm{dist}_a+\mathrm{dist}_{a\circ a}\geqslant n$ (by Lemma 4.1 that we are going to use without reference) and $2\,\mathrm{dist}_a+\mathrm{dist}_{a*a}\geqslant n$. Thus $\pi(a\circ a)$, $\pi(a*a)\geqslant n-(q-1)$ and we are free to choose one of the two distinct rows $a\circ a$, $a*a$ of $G\setminus K$. If $(a,b)\in S$ then $\mathrm{dist}_a+\mathrm{dist}_b+\mathrm{dist}_{a\circ b}\geqslant n$ and $\mathrm{dist}_a+\mathrm{dist}_b+\mathrm{dist}_{a*b}\geqslant n$. Since $a,b\in K$, we must have $a*b\in G\setminus K$, too, $\pi(a,b,a\circ b)$, $\pi(a,b,a*b)\geqslant n-(2m+q)$, and we are free to choose one of the two distinct rows $a\circ b$, $a*b$ of $G\setminus K$. Finally, if $(a,b)\in T$, then again $\mathrm{dist}_a+\mathrm{dist}_b+\mathrm{dist}_{a\circ b}\geqslant n$, $\mathrm{dist}_a+\mathrm{dist}_b+\mathrm{dist}_{a*b}\geqslant n$, we have $a\circ b\in K$, but we might have $a*b\in G\setminus K$. It is therefore better to consider the element $c=a^**(a\circ b)$ and the triple $(a,c,a*c)$ with respect to $G(*)$. Indeed, $a\in K$, $a*c=a\circ b\in K$, $b\neq c$ (since $a\circ b\neq a*b$), thus $a\circ c\neq a\circ b=a*a^**(a\circ b)=a*c$, $c\notin K$, and $(a,c)\in T(\circ,*)$. We then have $\pi(a,b,a\circ b)$, $\pi(a,c,a*c)\geqslant n-2m-q$ and we are free to choose one of the two alternatives.

Lemma 9.1. *Suppose that $(a_1,a_1),\dots,(a_\ell,a_\ell)\in R$ are distinct. Then $\pi\geqslant\ell(n-2q-m+1)$ provided that for $1\leqslant i\leqslant\ell$ there is $\cdot_i\in\{\circ,*\}$ such that $a_1\cdot_1 a_1,\dots,a_\ell\cdot_\ell a_\ell$ are distinct. In particular, this condition is always satisfied if n is odd or if $\ell=2$.*

Proof. For any a with $(a,a)\in R$ we have $\mathrm{dist}_a+\mathrm{dist}_a+\mathrm{dist}_{a\circ a}\geqslant n$ by Lemma 4.1. Since $a\in K$, it follows that $\mathrm{dist}_a+\mathrm{dist}_{a\circ a}\geqslant n-\mathrm{dist}_a\geqslant n-q+1$. Since (5.1) guaranteed only $m+q$ differences on the two rows a, $a\circ a$, the profit on these two rows is at least $n-q+1-(m+q)=n-2q-m+1$. A similar argument applies to the pair of rows a and $a*a$.

When $a_1\cdot_1 a_1,\dots,a_\ell\cdot_\ell a_\ell$ are distinct, we immediately obtain $\pi\geqslant\ell(n-2q-m+1)$ as $a_i\cdot_i a_i\in G\setminus K$ and $a_i\in K$ for all i. In particular, if n is odd we can choose $\cdot_i=\circ$ for all i, since the squaring map is a permutation in groups of odd order.

The case $\ell=2$ is resolved by a disjunction trick, using $a_2\circ a_2$ or a_2*a_2. □

Lemma 9.2. *Suppose that $r\geqslant 4$. Then $\pi\geqslant\min\{2(n-q-2m),3(n-2q-m+1)\}$.*

Proof. First suppose that there are $(a,a),(b,b)\in R$ such that $M=\{a\circ a,a*a,b\circ b,b*b\}$ satisfies $|M|\geqslant 3$. Pick any c such that $a\neq c\neq b$ and $(c,c)\in R$, which is possible since $r\geqslant 3$. If $c\circ c\notin M$ then $|\{a\cdot a,b\bullet b,c\circ c\}|\geqslant 3$ for some $\cdot,\bullet\in\{\circ,*\}$, and Lemma 9.1 implies $\pi\geqslant 3(n-2q-m+1)$. Let us therefore assume without loss of generality that $c\circ c=a\circ a$. Note that we then have $c\circ c\neq a*a$. If $c\circ c=b\circ b$ then $c\circ c\neq b*b$ and also $b*b\neq a*a$ (else $a\circ a=c\circ c=b\circ b$, $b*b=a*a$, $|M|<3$), so $a*a$, $c\circ c$, $b*b$ are distinct, and we are done by Lemma 9.1. If $c\circ c=b*b$ then $c\circ c\neq b\circ b$ and $b\circ b\neq a*a$ (else $b\circ b=a*a$, $b*b=c\circ c=a\circ a$, $|M|<3$), so $a*a$, $c\circ c$, $b\circ b$ are distinct, and we are done by Lemma 9.1. Thus we can assume $b\circ b\neq c\circ c\neq b*b$. Since either $a*a\neq b\circ b$ or $a*a\neq b*b$, the elements $c\circ c$, $a*a$, $b\cdot b$ are distinct for some $\cdot\in\{\circ,*\}$, and we finish with Lemma 9.1 again.

We can therefore suppose that there are $x,y\in G$ such that $\{a\circ a,a*a\}=\{x,y\}$ for every $(a,a)\in R$. Let $\rho=\min\{\mathrm{dist}_x,\mathrm{dist}_y\}$. Then for every $(a,a)\in R$ we have $\mathrm{dist}_a\geqslant(n-\rho)/2$, because $\mathrm{dist}_a+\mathrm{dist}_a+\mathrm{dist}_{a\cdot a}\geqslant n$ for $\cdot\in\{\circ,*\}$, and $\mathrm{dist}_{a\cdot a}\leqslant\rho$ for some $\cdot\in\{\circ,*\}$. The profit on the rows $\{a;\ (a,a)\in R\}\cup\{x,y\}$ is therefore at least $r((n-\rho)/2-m)+2(\rho-q)$. If $(n-\rho)/2-m\geqslant 0$, the assumption $r\geqslant 4$ yields profit at least $2(n-q-2m)$. Suppose that $(n-\rho)/2-m<0$. Then $\rho>n-2m$, so $\mathrm{dist}_{a\circ a}$, $\mathrm{dist}_{a*a}>n-2m$ for every $(a,a)\in R$. Let $(a,a),(b,b)\in R$ be distinct. Then there is $\cdot\in\{\circ,*\}$ such that $a\circ a$, $b\cdot b$ are distinct, and the profit on these rows is at least $2(n-2m-q+1)$. □

Lemma 9.3. *Suppose that $n=2p$ for some prime p. Then $\pi\geqslant\lceil r/2\rceil(n-2q-m+1)$.*

Proof. The only groups of order $2p$ are the cyclic group C_{2p} and the dihedral group D_{2p}. In these groups, for every $a\neq 1$ there are at most two elements b such that $a=b^2$. Hence there are at least

$\ell = \lceil r/2 \rceil$ distinct elements $(a_1, a_1), \ldots, (a_\ell, a_\ell) \in R$ with $a_1 \circ a_1, \ldots, a_\ell \circ a_\ell$ distinct. We are done by Lemma 9.1. □

Let us now establish several results concerning an upper bound on s.

Lemma 9.4. *Let $a \in K$ and let $b_1, \ldots, b_\ell \in K$ be distinct. Suppose that either $(a, b_1), \ldots, (a, b_\ell) \in S$, or $(b_1, a), \ldots, (b_\ell, a) \in S$. Then $\pi \geqslant \ell(n - 2q - m + 1) + q - m - 1$.*

Proof. Assume that $(a, b_1), \ldots, (a, b_\ell) \in S$, with the transposed situation being similar. By Lemma 4.1, for every i we have $\mathrm{dist}_{b_i} + \mathrm{dist}_{a \circ b_i} \geqslant n - \mathrm{dist}_a \geqslant n - q + 1$. Since $(a, b_i) \in S$, we have $a \neq b_i$ for every $1 \leqslant i \leqslant \ell$. Hence the elements $a, b_1, \ldots, b_\ell, a \circ b_1, \ldots, a \circ b_\ell$ are distinct, with $a \circ b_i \notin K$. The profit on a, b_1, $a \circ b_1$ is at least $n - (2m + q)$, while the profit on each of the $\ell - 1$ pairs of rows b_i, $a \circ b_i$ for $i > 1$ is at least $n - q + 1 - (m + q)$. □

Lemma 9.5. *If there are $(a, b), (c, d) \in S$ such that $|\{a, b, c, d\}| = 4$ then $\pi \geqslant 2(n - q - 2m)$.*

Proof. If $a \circ b \neq c \circ d$ then the profit at the distinct rows a, b, c, d, $a \circ b$, $c \circ d$ is at least $2(n - q - 2m)$, by Lemma 4.1. Otherwise use a disjunction trick and $c * d$ instead of $c \circ d$. □

Lemma 9.6. *If $s \geqslant 7$ then $\pi \geqslant 2(n - q - 2m)$.*

Proof. If there are three elements of S in the same row or in the same column, Lemma 9.4 implies $\pi \geqslant 3(n - 2q - m + 1) + (q - m - 1) \geqslant 2(n - q - 2m)$. Suppose that no three elements of S are in the same row or in the same column.

Define a multigraph Γ_S on K where $\{x, y\}$ is an edge if and only if $(x, y) \in S$ or $(y, x) \in S$. Then Γ_S has s edges, there are no more than two edges between any two vertices of S, and we claim that Γ_S has a 2-matching.

Suppose that Γ_S has a vertex x with two distinct neighbours y and z. By our assumptions on S, there are at most 4 edges incident with x. Also, there are at most 2 edges between y and z. Therefore if $s \geqslant 7$ then there is an edge disjoint from either $\{x, y\}$ or $\{x, z\}$, yielding the required 2-matching.

Alternatively, if no such x exists then edges are disjoint unless they join the same pair of vertices, and it is trivial to find a 2-matching.

Any 2-matching in Γ_S yields $\pi \geqslant 2(n - q - 2m)$ by Lemma 9.5. □

We are now going to establish results for t dual to Lemmas 9.4–9.6.

Lemma 9.7. *Let $a \in K$ and let $b_1, \ldots, b_\ell \notin K$ be distinct. Suppose that either $(a, b_1), \ldots, (a, b_\ell) \in T$, or that $(a_1, b_1), \ldots, (a_\ell, b_\ell) \in T$ for some $a_1, \ldots, a_\ell \in K$ such that $a_i \circ b_i = a$. Then $\pi \geqslant \ell(n - 2q - m + 1) + q - m - 1$.*

Proof. Let $(a, b_1), \ldots, (a, b_\ell) \in T$. By Lemma 4.1, for every i we have $\mathrm{dist}_{b_i} + \mathrm{dist}_{a \circ b_i} \geqslant n - \mathrm{dist}_a \geqslant n - q + 1$. We cannot have $a = a \circ b_i$ for some i, else $b_i = 1$, $(a, b_i) \notin \mathrm{diff}(\circ, *)$, so $(a, b_i) \notin T$. Hence the elements a, $b_1, \ldots, b_\ell$, $a \circ b_1, \ldots, a \circ b_\ell$ are distinct, with $a \circ b_i \in K$. The profit on a, b_1, $a \circ b_1$ is at least $n - (2m + q)$, while the profit on each of the $\ell - 1$ pairs of rows b_i, $a \circ b_i$ for $i > 1$ is at least $n - q + 1 - (m + q)$.

Now assume that $(a_i, b_i) \in T$, $a_i \circ b_i = a$ for some $a_i \in K$, $1 \leqslant i \leqslant \ell$. By Lemma 4.1, for every i we have $\mathrm{dist}_{a_i} + \mathrm{dist}_{b_i} \geqslant n - \mathrm{dist}_a \geqslant n - q + 1$. We cannot have $a = a_i$ for some i, else $a = a_i \circ b_i = a \circ b_i$, $b_i = 1$, $(a_i, b_i) \notin T$. Hence the elements a, $a_1, \ldots, a_\ell$, $b_1, \ldots, b_\ell$ are distinct. The profit on a_1, b_1, $a = a_1 \circ b_1$ is at least $n - (2m + q)$, while the profit on each of the $\ell - 1$ pairs of rows a_i, b_i for $i > 1$ is at least $n - q + 1 - (m + q)$. □

Lemma 9.8. *If there are $(a, b), (c, d) \in T$ such that $|\{a, c, a \circ b, c \circ d\}| = 4$ then $\pi \geqslant 2(n - q - 2m)$.*

Proof. If $b \neq d$ then $|\{a, b, c, d, a \circ b, c \circ d\}| = 6$ and we are done by Lemma 4.1. So let us assume that $b = d$. We can apply a disjunction trick and consider $e = c^* * (c \circ b) \in G \setminus K$, obtaining $e \neq b$, $\pi(c, e, c * e) \geqslant n - (2m + q)$. By our assumption, $\{a, a \circ b\} \cap \{c, c * e\} = \emptyset$. We therefore have additional profit of at least $n - (2m + q)$ on the rows a, b, $a \circ b$. □

Lemma 9.9. *If $t \geqslant 7$ then $\pi \geqslant 2(n - q - 2m)$.*

Proof. If there are three elements of T in the same row or with the same product, Lemma 9.7 implies $\pi \geqslant 3(n - 2q - m + 1) + (q - m - 1) \geqslant 2(n - q - 2m)$. Suppose that no three elements of T are in the same row or have the same product.

Define a multigraph Γ_T on K where $\{x, y\}$ is an edge if and only if there is z such that either $(x, z) \in T$ and $x \circ z = y$, or $(y, z) \in T$ and $y \circ z = x$. Then Γ_T has t edges and there are no more than two edges between any two vertices of T. Arguing as in the proof of Lemma 9.6, we can show that Γ_T has a 2-matching.

Hence there are $(a, b), (c, d) \in T$ such that $|\{a, c, a \circ b, c \circ d\}| = 4$, and we are done by Lemma 9.8. □

Finally, we return to the graph Γ_U based on the set U.

Lemma 9.10. *If Γ_U has a rainbow ℓ-matching then $\pi \geqslant \ell(n - 2q - m)$.*

Proof. The existence of a rainbow ℓ-matching in Γ_U is equivalent to the existence of ℓ pairwise disjoint sets $\{a_i, b_i, a \circ b_i\}$, where $(a_i, b_i) \in U$, so $a_i \in K$, b_i, $a \circ b_i \in G \setminus K$. The rest follows from Lemma 4.1. □

To illustrate the procedure outlined at the beginning of this section, let us eliminate $(n, h, k, m) = (24, 1, 16, 3)$. Since $\delta_0(24) = 120$, $q = \lceil n/3 \rceil = 8$, and $(n - k)q + (k - h)m = 109$, we need a profit of at least 12. Lemma 9.1 with $r = 2$ (thus $\ell = 2$) yields precisely $\pi \geqslant 12$. We can therefore assume $r \leqslant 1$, which Lemma 9.2 cannot improve. Lemma 9.4 yields a sufficient $\pi \geqslant 16$ with $\ell = 2$ (but $\ell = 1$ does not suffice), so $s \leqslant 1(k - h) = 15$. Since Lemma 9.6 yields $\pi \geqslant 20$, we can improve the bound to $s \leqslant 6$. Similarly, Lemma 9.7 with $\ell = 2$ yields $t \leqslant 15$, which Lemma 9.9 improves with $\pi \geqslant 20$ to $t \leqslant 6$. Then (8.2) allows us to assume that $u \geqslant 3(k - h) - 1 - 6 - 6 = 32$, and thus that Γ_U has at least $\lceil 32/2 \rceil = 16$ edges. Since $\mu_3(n - k) = \mu_3(8) = 15$ by Proposition 8.1, Γ_U contains a rainbow 3-matching. Then $\pi \geqslant 3(n - 2q - m) = 15 > 12$ by Lemma 9.10, which is what we need, and $(24, 1, 16, 3)$ is eliminated.

A straightforward calculation shows that the only remaining cases of (5.7) are

$$\big(24, 1, \{17, 18\}, 3\big), \quad \big(25, 1, \{17, 18\}, 3\big), \quad (26, 1, 19, 3), \quad \big(27, 1, \{19, 20\}, 3\big). \tag{9.1}$$

For these surviving cases the above procedure at least yields upper bounds on r, s, t and a lower bound on u as follows:

$$\begin{aligned}
(24, 1, 17, 3): &\quad r \leqslant 3,\ s \leqslant 6,\ t \leqslant 6,\ u \geqslant 33,\\
(24, 1, 18, 3): &\quad r \leqslant 17,\ s \leqslant 34,\ t \leqslant 34,\ u \geqslant 0,\\
(25, 1, 17, 3): &\quad r \leqslant 2,\ s \leqslant 6,\ t \leqslant 6,\ u \geqslant 34,\\
(25, 1, 18, 3): &\quad r \leqslant 3,\ s \leqslant 6,\ t \leqslant 6,\ u \geqslant 36,\\
(26, 1, 19, 3): &\quad r \leqslant 6,\ s \leqslant 6,\ t \leqslant 6,\ u \geqslant 36,\\
(27, 1, 19, 3): &\quad r \leqslant 2,\ s \leqslant 6,\ t \leqslant 6,\ u \geqslant 40,\\
(27, 1, 20, 3): &\quad r \leqslant 3,\ s \leqslant 38,\ t \leqslant 38,\ u \geqslant 0.
\end{aligned}$$

10. Stubborn cases

It is easy to check that the profit obtained from a rainbow 3-matching in U is not sufficient to eliminate any of the cases (9.1). We will need more delicate profits, for instance obtained from a rainbow 2-matching in U and an element $(a,b)\in S$ such that a, b, $a\circ b$ are disjoint from the vertices and colors of the rainbow 2-matching. We start with two dual lemmas that in certain circumstances provide upper bounds on s and t.

Lemma 10.1. *If $s\geqslant 3$ and $q\geqslant m+1$ then $\pi\geqslant 2n-3q-3m+1$.*

Proof. If there are $(a,b),(c,d)\in S$ with $|\{a,b,c,d\}|=4$, we are done by Lemma 9.5 and $q\geqslant m+1$. Otherwise there are $(a,b),(c,d)\in S$ with $|\{a,b,c,d\}|=3$. If either $a=c$ and $b\neq d$, or $a\neq c$ and $b=d$, then $\pi\geqslant 2n-3q-3m+1$ by Lemma 9.4 with $\ell=2$. The cases when $a=d$ or $b=c$ yield the same profit by an argument similar to Lemma 9.4. We cannot have $a=b$ or $c=d$ by the definition of S. □

Lemma 10.2. *If $t\geqslant 3$ and $q\geqslant m+1$ then $\pi\geqslant 2n-3q-3m+1$.*

Proof. If there are $(a,b),(c,d)\in T$ with $|\{a,c,a\circ b,c\circ d\}|=4$, we are done by Lemma 9.8 and $q\geqslant m+1$. Otherwise there are $(a,b),(c,d)\in T$ with $|\{a,c,a\circ b,c\circ d\}|=3$. The cases when $a=c$ or $a\circ b=c\circ d$ are handled by Lemma 9.7.

If either $a=c\circ d$ or $c=a\circ b$, we can assume without loss of generality that $a=c\circ d$. If $b\neq d$ then a, b, c, d, $a\circ b$ are distinct, and the profit on the rows a, b, $a\circ b$ is at least $n-(2m+q)$. Since $\mathrm{dist}_c+\mathrm{dist}_d\geqslant n-\mathrm{dist}_{c\circ d}\geqslant n-q+1$, the profit on the rows c, d is at least $n-2q-m+1$, and the total profit is at least $2n-3q-3m+1$.

Finally suppose that $a=c\circ d$, $b=d$, and the elements a, b, c, $a\circ b$ are distinct. Using a disjunction trick for (a,b), let us consider $(a,e=a^*\ast(a\circ b))\in T$ and $(c,b=d)\in T$, focusing on the rows a, e, $a\ast e=a\circ b$, c, $b=d$, $c\circ d$, which are distinct, except that $a=c\circ d$. We finish as above. □

Lemma 10.3. *We have $u\leqslant(n-k)(n-k-1)$.*

Proof. An element $(c,d)\in U$ determines the ordered pair $(d,c\circ d)\in(G\setminus K)\times(G\setminus K)$ with $d\neq c\circ d$ (since $c\neq 1$) and vice versa. □

We now elaborate on the idea of rainbow matchings in U disjoint from elements of R, S and/or T.

For $(a,b)\in R\cup S\cup T$, let $U\setminus\setminus(a,b)=\{(c,d)\in U;\ \{c,d,c\circ d\}\cap\{a,b,a\circ b\}=\emptyset\}$. For $(a,b),(c,d)\in R\cup S\cup T$, let $U\setminus\setminus(a,b)(c,d)=\{(e,f)\in U;\ \{a,b,a\circ b,c,d,c\circ d\}\cap\{e,f,e\circ f\}=\emptyset\}$.

Lemma 10.4. *For $(a,b)\in R\cup S\cup T$, we have*

$$\big|U\setminus\setminus(a,b)\big|\geqslant\begin{cases}u-(2n-2k+1), & \text{if } (a,b)\in R,\\ u-(2n-2k+4), & \text{if } (a,b)\in S\cup T.\end{cases}$$

Proof. Assume that $(a,b)\in S$. Then an element $(c,d)\in U$ does not belong to $U\setminus\setminus(a,b)$ if and only if one of the following occurs: $c=a$, $c=b$, $d=a\circ b$, $c\circ d=a\circ b$. Now, $c=a$ can occur for at most 2 elements of U, by the definition of U, given that row a contains $(a,b)\in S$. We have $c=b$ at most 3 times. We have $d=a\circ b$ at most $n-k$ times, because the column $a\circ b$ contains at most $n-k$ values from $G\setminus K$. Finally, $c\circ d=a\circ b$ occurs at most another $n-k-1$ times, because the value $a\circ b$ can occur at most once in every column of $G\setminus K$, and we have already accounted for all elements of U in column $a\circ b$. The result for $(a,b)\in S$ follows.

Assume that $(a,b)\in T$. Then an element $(c,d)\in U$ does not belong to $U\setminus\setminus(a,b)$ if and only if one of the following occurs: $c=a$, $c=a\circ b$, $d=b$, $c\circ d=b$. The rest is analogous to the case $(a,b)\in S$.

Assume that $(a,b) = (a,a) \in R$. Then an element $(c,d) \in U$ does not belong to $U \setminus\setminus (a,b)$ if and only if one of the following occurs: $c = a$, $d = a \circ a$, $c \circ d = a \circ a$. The rest is analogous to the case $(a,b) \in S$. □

Lemma 10.5. *If $(a,b),(c,d) \in S \cup T$ then $|U \setminus\setminus (a,b)(c,d)| \geqslant u - (4n - 4k + 8)$. If $(a,b),(c,d) \in S$ and $|\{a,b,c,d\}| = 3$ then $|U \setminus\setminus (a,b)(c,d)| \geqslant u - (4n - 4k + 5)$.*

Proof. For $(a,b),(c,d) \in S \cup T$, apply a variation of Lemma 10.4 twice. The worst case estimate $|U \setminus\setminus (a,b)(c,d)| \geqslant u - (4n - 4k + 8)$ is obtained when $|\{a,b,a \circ b,c,d,c \circ d\}| = 6$.

Suppose that $(a,b),(c,d) \in S$ and $|\{a,b,c,d\}| = 3$. An element $(e,f) \in U$ does not belong to $U \setminus\setminus (a,b)(c,d)$ if and only if one of the following occurs: $e \in \{a,b,c,d\}$, $f \in \{a \circ b, c \circ d\}$, or $e \circ f \in \{a \circ b, c \circ d\}$. Since $|\{a,b,c,d\}| = 3$, we can assume without loss of generality that either $a = c$, b, d are distinct, or $a = d$, b, c are distinct. (Note that $a = b$ is impossible since $(a,b) \in S$.) If $a = c$, b, d are distinct, then $e = a$ occurs at most once (since $(a,b),(c,d) \in S$), $e = b$ at most 3 times, and $e = d$ at most 3 times. If $a = d$, b, c are distinct, then $e = a$ occurs at most twice, $e = b$ at most 3 times, and $e = c$ at most twice. Hence in both cases, $e \in \{a,b,c,d\}$ occurs for at most 7 elements $(e,f) \in U$.

As before, we eliminate up to $2(n-k)$ elements $(e,f) \in U$ with $f \in \{a \circ b, c \circ d\}$, and a further $2(n-k-1)$ with $e \circ f \in \{a \circ b, c \circ d\}$. □

Note that in all cases (9.1) we have $k > 2n/3$. The following lemma will therefore apply to these cases.

Lemma 10.6. *Assume that $n \geqslant 12$ and $k > 2n/3$. Then $r + s > 0$ or $G(\circ)$, $G(*)$ are isomorphic via a transposition.*

Proof. Assume that $r + s = 0$. The proof of [3, Proposition 3.1] (our Proposition 4.7) goes through with $k > 2n/3$ (rather than $k > 3n/4$), except for part (iv), as explicitly noted already by Drápal in [3]. With our assumption $r + s = 0$, we can replace the proof of (iv) with the following: Let $g \in G$. Then there are $a, b \in K$ such that $g = a \circ b$, since $k > n/2$. Assume $g = a_i \circ b_i$ for some $a_i, b_i \in K$, $1 \leqslant i \leqslant 2$. If $a_1 * b_1 \neq a_2 * b_2$ then there is i such that $a_i \circ b_i \neq a_i * b_i$, and for this i we have $(a_i, b_i) \in R \cup S$, a contradiction. Thus $a_1 * b_1 = a_2 * b_2$.

We can now conclude from [3, Proposition 3.1] that there is an isomorphism $f : G(\circ) \to G(*)$ such that $f(a) = a$ for every $a \in K$. Then by [3, Proposition 6.1], $\operatorname{dist}(\circ, *) \geqslant \delta_0(\circ)$, and if equality holds, f must be a transposition. □

The following example shows that Lemma 10.6 is best possible. Let $\circ, *$ be defined by

$\circ$	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	5	6	4	8	9	7
3	3	1	2	6	4	5	9	7	8
4	4	5	6	7	8	9	1	2	3
5	5	6	4	8	9	7	2	3	1
6	6	4	5	9	7	8	3	1	2
7	7	8	9	1	2	3	4	5	6
8	8	9	7	2	3	1	5	6	4
9	9	7	8	3	1	2	6	4	5

$*$	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	5	6	4	8	9	7
3	3	1	2	6	4	5	9	7	8
4	4	5	6	7	8	9	2	3	1
5	5	6	4	8	9	7	3	1	2
6	6	4	5	9	7	8	1	2	3
7	7	8	9	2	3	1	5	6	4
8	8	9	7	3	1	2	6	4	5
9	9	7	8	1	2	3	4	5	6

where the differences are shaded. Then $k = 2n/3$ and yet the groups are not isomorphic; $G(\circ) \cong (C_3)^2$ and $G(*) \cong C_9$. By taking direct products of these two groups with other groups we can make arbitrarily large non-isomorphic pairs where $k = 2n/3$ and $r = s = 0$.

Lemma 10.7. *Suppose that $k = n - q + 2$ and $x, y \in G \setminus K$, $x \neq y$. Then there is $(v,w) \in \operatorname{diff}(\circ, *)$ such that $\{v, w, v \circ w\} \cap \{x, y\} = \emptyset$, $v \in G \setminus K$, and either $w \in K$ or $v \circ w \in K$.*

Proof. The set $L = G \setminus (K \cup \{x, y\})$ is not closed under $\circ$ since it does not contain 1, so there are $v, w \in L$ such that $v \circ w \notin L$. If $v \circ w \in K$, we are done. Otherwise $v \circ w \in \{x, y\}$, and we can assume without loss of generality that $v \circ w = x$. Since $v \in G \setminus K$, $\mathrm{dist}_v \geqslant q = n - k + 2$, but $|(G \setminus K) \cup \{v^\circ \circ x, v^\circ \circ y\}| \leqslant n - k + 1$ (as $v^\circ \circ x = v^\circ \circ v \circ w = w \in G \setminus K$), so there is $z \in K$ with $(v, z) \in \mathrm{diff}(\circ, *)$, and $v \circ z \notin \{x, y\}$. Then $\{v, z, v \circ z\} \cap \{x, y\} = \emptyset$, $v \in G \setminus K$, $z \in K$, and (v, z) does the job. □

We now eliminate all the quadruples of (9.1), sorting them according to the difference $n - k$.

Case $(n, h, k, m) = (25, 1, 17, 3)$. To eliminate this case, we need a profit of at least $\delta_0(n) - (n-k)q - (k-h)m + 1 = 13$, and we can assume $r \leqslant 2$, $s \leqslant 6$, $u \geqslant 34$. If $s > 0$ and $(a, b) \in S$ then $|U \setminus\setminus (a, b)| \geqslant u - (2n - 2k + 4) \geqslant 14$ by Lemma 10.4, so there is $(c, d) \in U$ such that a, b, $a \circ b$, c, d, $c \circ d$ are distinct, yielding the profit of at least $(n - q - 2m) + (n - 2q - m) = 14 > 13$. We can therefore assume that $s = 0$ and $u \geqslant 40$. By Lemma 10.6, $r > 0$ and there is $(a, a) \in R$. Then $|U \setminus\setminus (a, a)| \geqslant u - (2n - 2k + 1) \geqslant 23$ by Lemma 10.4. Since $\mu_2(n - k) = \mu_2(8) = 8 \leqslant \lceil 23/2 \rceil$, there is a rainbow 2-matching in U disjoint from $\{a, a \circ a\}$, and we obtain a sufficient profit of at least $(n - 2q - m + 1) + 2(n - 2q - m) = 13$.

Case $(n, h, k, m) = (27, 1, 19, 3)$. We need a profit of at least 19, and we can assume $r \leqslant 2$, $s \leqslant 6$, $u \geqslant 40$. If $s > 0$ and $(a, b) \in S$ then $|U \setminus\setminus (a, b)| \geqslant u - (2n - 2k + 4) \geqslant 20$ by Lemma 10.4, $\mu_2(n - k) = \mu_2(8) = 8 \leqslant \lceil 20/2 \rceil$, so there is a rainbow 2-matching disjoint from $\{a, b, a \circ b\}$, yielding a sufficient profit of $(n - q - 2m) + 2(n - 2q - m) = 24$. We can therefore assume that $s = 0$ and $u \geqslant 46$. By Lemma 10.6, $r > 0$ and there is $(a, a) \in R$. Then $|U \setminus\setminus (a, a)| \geqslant u - (2n - 2k + 1) \geqslant 29$ by Lemma 10.4. Since $\mu_2(n - k) = 8 \leqslant \lceil 29/2 \rceil$, there is a rainbow 2-matching disjoint from $\{a, a \circ a\}$, and we obtain a sufficient profit of at least $(n - 2q - m + 1) + 2(n - 2q - m) = 19$.

Case $(n, h, k, m) = (24, 1, 17, 3)$. We need a profit of at least 17, and we can assume $r \leqslant 3$, $s \leqslant 6$, $t \leqslant 6$, $u \geqslant 33$. If $s > 0$ and $(a, b) \in S$ then $|U \setminus\setminus (a, b)| \geqslant 15$ by Lemma 10.4, $\mu_2(n - k) = \mu_2(7) = 7 \leqslant \lceil 15/2 \rceil$, so there is a rainbow 2-matching in U disjoint from $\{a, b, a \circ b\}$, for a sufficient profit of at least $(n - q - 2m) + 2(n - 2q - m) = 20$. Similarly if $t > 0$. We can therefore assume that $s = 0$, $t = 0$ and $u \geqslant 45$. There is $(a, a) \in R$ by Lemma 10.6, $|U \setminus\setminus (a, a)| \geqslant 30$ by Lemma 10.4, $\mu_3(n - k) = \mu_3(7) = 15 = \lceil 30/2 \rceil$, so there is a rainbow 3-matching in U disjoint from $\{a, a \circ a\}$, giving a sufficient profit of at least $(n - 2q - m + 1) + 3(n - 2q - m) = 21$.

Case $(n, h, k, m) = (26, 1, 19, 3)$. We need a profit of at least 20, and we can assume $r \leqslant 6$, $s \leqslant 6$, $t \leqslant 6$, $u \geqslant 36$. If $s > 0$ and $(a, b) \in S$ then $|U \setminus\setminus (a, b)| \geqslant 18$ by Lemma 10.4, $\mu_2(n - k) = \mu_2(7) = 7 \leqslant \lceil 18/2 \rceil$, so there is a rainbow 2-matching in U disjoint from $\{a, b, a \circ b\}$, for a sufficient profit of at least $(n - q - 2m) + 2(n - 2q - m) = 21$. Similarly if $t > 0$. If $s = 0 = t$ then $u \geqslant 52$, a contradiction of Lemma 10.3, which yields $u \leqslant 42$.

Case $(n, h, k, m) = (25, 1, 18, 3)$. We need a profit of at least 19, and we can assume $r \leqslant 3$, $s \leqslant 6$, $t \leqslant 6$, $u \geqslant 36$. Suppose that $s \geqslant 3$. If there are $(a, b), (c, d) \in S$ such that $|\{a, b, c, d\}| = 4$ then Lemma 9.5 yields a sufficient profit of at least $2(n - q - 2m) = 20$. Otherwise, as in the proof of Lemma 10.1, there are $(a, b), (c, d) \in S$ such that $|\{a, b, c, d\}| = 3$ and $\pi(a, b, c, d, a \circ b, c \circ d) \geqslant 2n - 3q - 3m + 1 = 15$. Moreover, Lemma 10.5 implies that $|U \setminus\setminus (a, b)(c, d)| \geqslant 3$, so there is $(e, f) \in U$ such that $\{e, f, e \circ f\} \cap \{a, b, c, d, a \circ b, c \circ d\} = \emptyset$. Since $\pi(e, f, e \circ f) \geqslant n - 2q - m = 4$, we have $\pi \geqslant 15 + 4 = 19$, as desired. We can therefore assume that $s \leqslant 2$ and $u \geqslant 40$. Using Lemma 10.5 once more, we may now deduce that $t \leqslant 2$. Hence $u \geqslant 44$, contradicting $u \leqslant 42$ from Lemma 10.3.

Case $(n, h, k, m) = (27, 1, 20, 3)$. We need a profit of at least 25, and we can assume $r \leqslant 3$. Suppose that $s \geqslant 7$. Then by Lemma 9.6, there are $(a, b), (c, d) \in S$ such that $\pi(a, b, c, d, a \circ b, c \circ d) \geqslant 2(n - q - 2m) = 24$. Using $(x, y) = (a \circ b, c \circ d)$ in Lemma 10.7, we obtain $(v, w) \in \mathrm{diff}(\circ, *)$ such that $\{v, w, v \circ w\} \cap \{x, y\} = \emptyset$, $v \in G \setminus H$, and either $w \in K$ or $v \circ w \in K$. We have not yet used any of the rows v, w, $v \circ w$ that happen to be in $G \setminus K$ in our calculation of the profit. We have therefore counted at most $q + q + (q - 1) = 3q - 1$ differences on the rows v, w, $v \circ w$ so far, however, we have $\mathrm{dist}_v + \mathrm{dist}_w + \mathrm{dist}_{v \circ w} \geqslant n = 3q$ because $(v, w) \in \mathrm{diff}(\circ, *)$. We can now increase the profit of 24 by 1, and we are done. Similarly, if $t \geqslant 7$, there are $(a, b), (c, d) \in T$ such that $\pi(a, b, c, d, a \circ b, c \circ d) \geqslant 24$ by Lemma 9.7, and we can apply Lemma 10.7 with $(x, y) = (b, d)$ to increase the profit by 1. We can therefore assume $s \leqslant 6$, $t \leqslant 6$ and $u \geqslant 42$. If $s \geqslant 3$, there are $(a, b), (c, d) \in S$ with $\pi(a, b, c, d, a \circ b, c \circ d) \geqslant 2n - 3q - 3m + 1 = 19$ by Lemma 10.1, $|U \setminus\setminus (a, b)(c, d)| \geqslant 6$ by Lemma 10.5, $(e, f) \in U$ with $\{e, f, e \circ f\} \cap \{a, b, c, d, a \circ b, c \circ d\} = \emptyset$, and $\pi(e, f, e \circ f) \geqslant n - 2q - m = 6$, for a sufficient profit of $19 + 6 = 25$. We can therefore assume $s \leqslant 2$ and $u \geqslant 46$, contradicting $u \leqslant 42$ from Lemma 10.3.

Case $(n,h,k,m) = (24,1,18,3)$. We need a profit of at least 22.

Define λ to be the maximum integer for which there exist distinct $x, y \in G$ such that $\mathrm{dist}_x \geqslant \mathrm{dist}_y \geqslant \lambda$. Suppose that $\lambda \geqslant 17$. By Lemma 10.7 there is $(v,w) \in \mathrm{diff}(\circ,*)$ with $\{v, w, v\circ w\} \cap \{x,y\} = \emptyset$ and $|K \cap \{w, v\circ w\}| \geqslant 1$ so $\pi(v,w,v\circ w,x,y) \geqslant n - 2q - m + 2(\lambda - q) \geqslant 23$. Thus we may assume that $\lambda \leqslant 16$.

Let Ω be a maximal subset of $R \cup S \cup T$ under the constraint that there should be a maximum of 3 elements of Ω within any row. Let Σ be the sum over Ω of $\mathrm{dist}_a + \mathrm{dist}_b - 2m$ for elements $(a,b) \in R \cup S$, and $\mathrm{dist}_a + \mathrm{dist}_{a\circ b} - 2m$ for $(a,b) \in T$.

We claim that $\Sigma \geqslant |\Omega|(n - 2m - \lambda)$. Each $(a,b) \in R \cup S$ satisfies $\mathrm{dist}_a + \mathrm{dist}_b \geqslant n - \min\{\mathrm{dist}_{a\circ b}, \mathrm{dist}_{a*b}\} \geqslant n - \lambda$. So it suffices to show that each $(a,b) \in T$ satisfies $\mathrm{dist}_a + \mathrm{dist}_{a\circ b} \geqslant n - \lambda$. Since $(a,b) \in T$, we have $\mathrm{dist}_a + \mathrm{dist}_{a\circ b} \geqslant n - \mathrm{dist}_b$. By a disjunction trick, $(a,c) \in T$ where $c = a^* * (a \circ b)$, so $\mathrm{dist}_a + \mathrm{dist}_{a\circ b} \geqslant n - \mathrm{dist}_c$. Since b, c are distinct elements of $G \setminus K$, we have $\lambda \leqslant \min\{\mathrm{dist}_b, \mathrm{dist}_c\}$, from which the claim follows.

Next we claim that $\Sigma \leqslant 8(37 - 2\lambda)$. Consider $a \in K \setminus H$. By construction, a is a row coordinate for at most 3 cells in Ω. By Lemma 9.4, there are at most 2 cells in S for which a is the column coordinate, otherwise we realize a sufficient profit of $3(n - 2q - m + 1) + q - m + 1 = 24$. Similarly, using Lemma 9.7, there are at most 2 cells (c,d) in T for which $a = c \circ d$. It is also possible that a is the column coordinate for a single cell in R. It follows that $\Sigma \leqslant 8\Sigma'$, where Σ' is the sum over $a \in K \setminus H$ of $\mathrm{dist}_a - m$. As the profit from $K \cup \{x,y\}$ is at least $\Sigma' + 2(\lambda - q)$ we are done unless $\Sigma' \leqslant 21 + 2q - 2\lambda = 37 - 2\lambda$. This proves the claim.

Combining the previous two claims we find that $|\Omega| \leqslant 8(37-2\lambda)/(n-2m-\lambda) = 16 + 8/(18-\lambda) \leqslant 20$, since $\lambda \leqslant 16$. As $\Omega \cup U$ contains three differences in every row indexed by $K \setminus H$, it follows that $u \geqslant 3(k-h) - |\Omega| \geqslant 31$. This contradicts Lemma 10.3, finishing the last case.

11. Constructions

We have now established all distances mentioned in Theorem 2.1. It remains to present the constructions that realize the minimal distances $\delta(\circ) = \mathrm{dist}(\circ,*)$ in situations when $\delta(\circ) < \delta_0(\circ)$.

11.1. Cyclic and dihedral constructions

The following two constructions (11.1) and (11.2) were introduced in [8]. Given a certain group $G(\circ)$ of even order n, they produce a group $G(*)$ at distance $n^2/4$ from $G(\circ)$.

Recall the graphs $\mathcal{G}(n)$ and $\mathcal{G}'(n)$ from the Introduction. It turns out that whenever two groups $G(\circ)$, $G(*)$ of order $n = 8$ or $n = 16$ are at distance $n^2/4$, there is a group $G(\cdot)$ obtained from $G(\circ)$ by one of the two constructions and such that $G(*) \cong G(\cdot)$. This follows from the fact that the graph $\mathcal{G}(8)$ (calculated in [17] and independently here) coincides with $\mathcal{G}'(8)$, and from the fact that the graph $\mathcal{G}(16)$ (calculated here for the first time) coincides with $\mathcal{G}'(16)$ (calculated by Bálek [1] and independently here).

For a fixed positive integer m and the set $M = \{-m+1, -m+2, \ldots, m-1, m\}$, define $\sigma : \mathbb{Z} \to \{-1, 0, 1\}$ by

$$\sigma(i) = \begin{cases} 1, & i > m, \\ 0, & i \in M, \\ -1, & i < 1 - m. \end{cases}$$

The cyclic construction. Let $G(\circ)$ be a group of order n, $S \leqslant G$, $G/S = \langle\alpha\rangle$ a cyclic group of order $2m$ and $1 \neq h \in S \cap Z(G)$. Then $G(\circ)$ is the disjoint union $\bigcup_{i\in M} \alpha^i$, and we can define a new multiplication $*$ on G by

$$x * y = x \circ y \circ h^{\sigma(i+j)}, \tag{11.1}$$

where $x \in \alpha^i$, $y \in \alpha^j$, and $i, j \in M$. Then $G(*)$ is a group and $\mathrm{dist}(\circ,*) = n^2/4$.

The dihedral construction. Let $G(\circ)$ be a group of order n, $S \trianglelefteq G$, G/S a dihedral group of order $4m$ (where we allow $m = 1$), and β, γ involutions of G/S such that $\alpha = \beta\gamma$ is of order $2m$. Let $G_0 = \bigcup_{i\in M} \alpha^i$ and $G_1 = G \setminus G_0$. Let $1 \neq h \in S \cap Z(G_0)$ be such that $hxh = x$ for some (and hence every) $x \in G_1$. Then there are $e \in \beta$ and $f \in \gamma$ so that G is the disjoint union $\bigcup_{i\in M}(\alpha^i \cup e\alpha^i)$ or $\bigcup_{j\in M}(\alpha^j \cup \alpha^j f)$, and we can define a new multiplication $*$ on G by

$$x * y = x \circ y \circ h^{(-1)^r \sigma(i+j)}, \tag{11.2}$$

where $x \in \alpha^i \cup e\alpha^i$, $y \in (\alpha^j \cup \alpha^j f) \cap G_r$, $i, j \in M$, and $r \in \{0, 1\}$. Then $G(*)$ is a group and $\operatorname{dist}(\circ, *) = n^2/4$.

11.2. Other constructions

The following three constructions furnish the distances of Theorem 2.1 with $\operatorname{dist}(\circ, *) < \delta_0(\circ)$ and $n \neq 2^k$.

Construction 1. Suppose $n \equiv 2 \bmod 4$ and $n \geqslant 6$. Let O be an abelian group of order $n/2$. We have two groups defined on the set $O \times C_2$, namely $D(O)$ and the usual direct product on $O \times C_2$. The distance between these two groups is $n(n-2)/2$. When $n \in \{6, 10\}$, this is $\delta(D_n)$ so $\Delta(D_n)$ contains a group isomorphic to $C_{n/2} \times C_2 \cong C_n$ (although $\Delta(D_{10})$ also contains a group isomorphic to D_{10}, because $n(n-2)/2 = 6n - 20 = \delta_0(D_{10})$).

Construction 2. We construct two abelian group operations $\odot$, $\circledast$ on the set $C_a \times C_b$ where a is odd.

$$(s, t) \odot (u, v) = \begin{cases} (s + u, t + v + 1), & \text{if } s + u \geqslant a, \\ (s + u, t + v), & \text{otherwise.} \end{cases}$$

Clearly $\odot$ is isomorphic to C_{ab} by the map $(s, t) \mapsto s + at$.

To form $\circledast$ we take the usual group on $C_a \times C_b$ and apply the isomorphism

$$(s, t) \mapsto \begin{cases} (s, t + 1), & \text{if } s \geqslant \frac{1}{2}(a + 1), \\ (s, t), & \text{otherwise.} \end{cases}$$

It is routine to check that $d(\odot, \circledast) = n^2(1 - a^{-2})/4$. In particular, $d(\odot, \circledast) = 2n^2/9$ when $a = 3$, the nearest (proportional) distance between non-isomorphic groups [13]. Note that $2n^2/9 < \delta_0(n)$ for $n \leqslant 21$, and indeed $\delta(C_{3b}) = 2n^2/9$ for $2 \leqslant b \leqslant 7$. The above construction proves this for $b \in \{2, 4, 5, 7\}$.

Construction 2 shows directly that the following achieve $2n^2/9$:

$$\operatorname{dist}(C_6, C_6), \quad \operatorname{dist}\big(C_9, C_3^2\big), \quad \operatorname{dist}(C_{12}, C_{12}), \quad \operatorname{dist}(C_{15}, C_{15}),$$
$$\operatorname{dist}(C_{18}, C_6 \times C_3), \quad \operatorname{dist}(C_{21}, C_{21}).$$

Taking appropriate extensions of the example that realizes $\operatorname{dist}(C_6, C_6)$, we can show that $2n^2/9$ is also achieved in these cases:

$$\operatorname{dist}(C_6 \times C_2, C_6 \times C_2), \quad \operatorname{dist}(C_6 \times C_3, C_6 \times C_3), \quad \operatorname{dist}(D_{12}, D_{12}), \quad \operatorname{dist}(\mathrm{Dic}_{12}, \mathrm{Dic}_{12}).$$

Similarly, $\operatorname{dist}(D_{18}, (C_3)^2 \rtimes C_2)$ is achieved by an extension of the example that yields $\operatorname{dist}(C_9, (C_3)^2)$. The above is a complete catalogue of cases where two groups are at distance precisely $2n^2/9$, except for the ad hoc constructions for $\operatorname{dist}(C_9, C_9)$, $\operatorname{dist}(C_{18}, C_{18})$ and $\operatorname{dist}(D_{18}, D_{18})$ below.

Construction 2 can also be used directly to realize $\operatorname{dist}(C_{10}, C_{10})$ and $\operatorname{dist}(C_{14}, C_{14})$.

Construction 3. (*Ad hoc*)

$\operatorname{dist}(C_7, C_7)$: The distance between $C_7 = \{0, \ldots, 6\}$ and its (12)(56) isomorph is 18.

$\operatorname{dist}(C_9, C_9)$: The distance between $C_9 = \{0, \ldots, 8\}$ and its (36)(47)(58) isomorph is $2n^2/9 = 18$.

Appropriate extensions of this last example realize both $\mathrm{dist}(C_{18}, C_{18})$ and $\mathrm{dist}(D_{18}, D_{18})$.

Remark 11.1. The computer calculations used in this paper were as follows: The graphs $\mathcal{G}'(8)$ and $\mathcal{G}'(16)$ were calculated by the first author using the GAP [12] package LOOPS [15] and modified code from [19]. The inequalities of Section 5 were independently verified by both authors, resulting in the list (5.7). The algorithm for $m = 2$ of Section 6.1 was implemented by both authors independently, and so was the algorithm for distances of cyclic groups of Section 6.2. The general algorithm for $\mathrm{dist}([\circ], [*])$ was run by the second author for all $n \leqslant 22$ (which took several months on a single processor computer), and by the first author for $n \leqslant 15$. Both authors verified the values $\mu_3(6)$–$\mu_3(10)$ of Proposition 8.1 with independent programs. Finally, the upper bounds on r, s, t and lower bounds on u of Section 9 were also performed independently by the two authors.

References

[1] M. Bálek, Grupy malých vzdáleností, M.S. thesis, Charles University, Prague, 2002 (in Czech).
[2] O. Chein, Moufang loops of small order. I, Trans. Amer. Math. Soc. 188 (1974) 31–51.
[3] A. Drápal, How far apart can the group multiplication tables be?, European J. Combin. 13 (1992) 335–343.
[4] A. Drápal, Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables, European J. Combin. 21 (2000) 301–321.
[5] A. Drápal, On distances of 2-groups and 3-groups, in: Groups St. Andrews 2001 in Oxford, vol. I, in: London Math. Soc. Lecture Note Ser., vol. 304, Cambridge Univ. Press, Cambridge, 2003, pp. 143–149.
[6] A. Drápal, Near 2-groups yield an isomorphism with many fixed points, Discrete Math. 266 (2003) 217–228.
[7] A. Drápal, On minimum distances of latin squares and the quadrangle criterion, Acta Sci. Math. (Szeged) 70 (2004) 3–11.
[8] A. Drápal, On groups that differ in one of four squares, European J. Combin. 23 (8) (2002) 899–918.
[9] A. Drápal, Cyclic and dihedral constructions of even order, Comment. Math. Univ. Carolin. 44 (4) (2003) 593–614.
[10] A. Drápal, P. Vojtěchovský, Moufang loops that share associator and three quarters of their multiplication tables, Rocky Mountain J. Math. 36 (2) (2006) 425–455.
[11] A. Drápal, N. Zhukavets, On multiplication tables of groups that agree on half of the columns and half of the rows, Glasg. Math. J. 45 (2) (2003) 293–308.
[12] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.4.12, http://www.gap-system.org, 2008.
[13] G. Ivanyos, F. Le Gall, Y. Yoshida, On the distance between non-isomorphic groups, preprint, European J. Combin., in press.
[14] B.D. McKay, nauty—Graph isomorphic software, http://cs.anu.edu.au/~bdm/nauty/.
[15] G.P. Nagy, P. Vojtěchovský, Loops: computing with quasigroups and loops in GAP, version 2.1.0, available at: http://www.math.du.edu/loops.
[16] G.P. Nagy, P. Vojtěchovský, The Moufang loops of order 64 and 81, J. Symbolic Comput. 42 (9) (2007) 871–883.
[17] P. Vojtěchovský, On Hamming distances of groups, M.S. thesis, Charles University, Prague, 1998 (in Czech).
[18] P. Vojtěchovský, Distances of groups of prime order, in: Proceedings of Olomouc Workshop on General Algebra '98, in: Contrib. Gen. Algebra, vol. 11, Verlag Johannes Heyn, Klagenfurt, 1999, pp. 225–231.
[19] P. Vojtěchovský, Toward the classification of Moufang loops of order 64, European J. Combin. 27 (3) (2006) 444–460.
[20] N. Zhukavets, On small distances between small 2-groups, Comment. Math. Univ. Carolin. 42 (2) (2001) 247–257.